SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT
[H2020 - Grant Agreement No. 700199]

Deliverable D6.4

Final Report on Exploitation Activities

Editor D. Katsianis (inCITES)

Contributors L. Jacquin (Hewlett Packard Labs), B. Gastón (I2CAT), I. Neokosmidis, Th. Rokkas, D. Katsianis (inCITES), A. Litke, D. Papadopoulos, N. Papadakis (INFILI), Christos Mathas, Anastasios Gogos (NCSR Demokritos), O.E. Segou (Orion Innovations PC), A. Lioy, M. De Benedictis (Politecnico di Torino), G. Gardikis, I. Mertzanis, S. Costicoglou, T. Michalakis (Space Hellas S.A.), G. Dimopoulos (TALAIA Networks), A. Pastor, J. Núñez, (Telefonica I+D), T. Batista, R. Preto (Ubiwhere)

Version 1.0

Date February 28th, 2019

Distribution PUBLIC (PU)

Executive Summary

The present document summarises the main findings and conclusions of the project activities related to the analysis of global cybersecurity market and environment, identification of SHIELD positioning in the market as well as the demonstration of the barriers that may hinder system's market acceptance. Furthermore, a detail techno-economic analysis survey about the offered services within the proposed technology has been presented. All these findings have resulted in updated per-partner individual exploitation plans for the project results as well as joint exploitation plans for selected cases.

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.

The overall growth in the cloud-based security services market is above that of the total information security market. Gartner estimates the cloud-based security services market will reach close to $9 billion by 2020. In addition, new available data from Gartner in 2018 confirms the trends in security market, where there will be an increase in security investments by 40 percent, partially caused by GDPR and privacy concerns related to the companies' digital transformation.

Our market survey acknowledges, based on 2019 data, the versatility of SHIELD, by the fact that it combines most of the capabilities of the other compared solutions, thanks to the distinctiveness of its architecture that allows for the synergy of different key components. The analysis indicates that there does not seem to exist a commercial and integrated solution offering both SOAR features and advanced mitigation capabilities focused on virtual network services.

On the other hand, SHIELD is a newcomer on a very competitive market, populated mostly by companies that are well-established in the cybersecurity domain. In order to maximise its adoption chances, SHIELD has to overcome a few major barriers that have been identified in this document. The aim should be that the selected business model (TSS - Telecom Security Service) overcomes most of the barriers by addressing the lock and trust in the vendor, leveraging the trust in the Operator.

The techno-economic analysis quantifies profitable business cases and opportunities for European players –mostly telcos- in collaboration with SMEs in the sector of NFV and Security Analytics, offering an advanced innovative blend of services. The results reveal that there are viable business cases for a target market segment of small/medium enterprises and with operators experiencing substantial market share (~30%) in typical large European countries. The TSS model could be profitable in most cases for established operators with reasonable market share, since the structure of the investment in IT and network components graduates according to the number of the clients and the traffic generated. The payback periods are generally around 5 years, which is not considered too long against the magnitude of the project. The possible revenues for technology provider SMEs specialized in NFV technology, vNSF developers and Data Analytics specialists are identified.

Sensitivity analysis has been carried out in order to rank a number of selected uncertainty assumption variables according to their impact on the NPV. Risk analysis has been carried out for the improvement of the analysis. For our scenarios, we have calculated the minimum monthly ARPU required for NPV to be equal to zero at the end of the study period. It is also seen that TSS Operators in highly competitive markets with a market share below 10% may experience problems in proposing a viable business plan. The total OPEX cost, as expected, is more critical for the total NPV compared to CAPEX, since the contribution of OPEX cost in the total investment cost is more than 3/4 of the total yearly costs. Likewise, the percentiles analysis shows that 50% of the NPVs values are greater that the base value calculations presented in the base case scenarios.

All the above mentioned conclusions, as well as the lessons learnt from the Y2 activities, helped the SHIELD partners to update their exploitation plans and also present viable joint exploitation plans, better positioning their ambition with respect to the quantified project results.

Table of Contents

1. INTRODUCTION 6
2. MARKET ANALYSIS 7
2.1. Evolution of the market 7
2.2. Possible competitors 9
2.3. Product Comparison 9
2.4. Barriers for SHIELD 15
2.5. SWOT and Business Modelling Analysis 16
3. TECHNO ECONOMIC ANALYSIS 20
3.1. Techno-economic Framework 20
3.2. Forecast and traffic estimations 23
3.2.1. Subscribers Forecast and Market Definition 23
3.2.2. Traffic Calculations 27
3.2.3. Financial Assumptions 29
3.2.4. Service Definition and Revenue estimations 29
3.3. Scenario Definition - Deployment - Architecture 31
3.3.1. Dimensioning rules per Case 32
3.3.2. Cost estimations 33
3.3.3. CAPEX estimations 33
3.3.4. OPEX estimations 34
3.4. Results and Analysis 36
3.4.1. Sensitivity Analysis 41
3.4.2. Risk Analysis 45
4. EXPLOITATION PLANS 48
4.1. SHIELD final results and owners 48
4.2. Join Exploitation Plans 49
4.2.1. Joint exploitation plan for the SHIELD offering as the TSS enabler platform 49
4.2.2. HPELB-POLITO-TID joint exploitation plan: Trust Monitor as-a-Service 50
4.2.3. HPELB-POLITO joint exploitation plan: vTPM development 50
4.3. Individual Exploitation Plans 51
4.3.1. HPELB 51
4.3.2. I2CAT 51
4.3.3. inCITES 52

4.3.4. INFILI 52
4.3.5. NCSRD 53
4.3.6. ORION 53
4.3.7. POLITO 54
4.3.8. SPH 54
4.3.9. TALAIA 55
4.3.10. TID 55
4.3.11. UBI 56
5. CONCLUSIONS 58
REFERENCES 59
LIST OF ACRONYMS 60
APPENDIX A. SHIELD USE CASES DESCRIPTION 63

1. INTRODUCTION

This Deliverable provides the final report on SHIELD exploitation activities including: recent updates of global cybersecurity market and environment; identification of SHIELD positioning in the market and its unique value proposition with its barriers; financial and economic analysis; as well as sensitivity and risk analysis in order to assess technology and market risks. Furthermore, strategic guidelines for the most appropriate services for development have been provided. In addition, joint exploitation plans and individual exploitation plans are identified.

WP6 "Commercial outreach, branding and exploitation" is responsible, among others, to maximize the internal exploitation of the SHIELD platform among the partners; to expand the adoption of the SHIELD platform; and to maximize the impact of SHIELD in the cybersecurity community. The relevant task T6.3 "Exploitation of innovation and technological results", whose work is partially reflected in the present document, includes the following subtasks: i) a market analysis describing the main competitors of SHIELD platform and how to effectively compete with them, ii) a roadmap to maximize the chances of SHIELD commercialization in the different market segments and, iii) techno-economic analysis (business plans) where profitable business cases and opportunities for European players via advanced innovative solutions must be analysed. Deliverable D6.4 addresses the last point.

This document is organised in three sections: in the first section, the SHIELD positioning in the market including the evolution of the market, the description and the evaluation of the possible competitors, the entry barriers for the systems as well as connection of the Business Model with financial analysis, are presented. In the second part, a detailed techno-economic analysis identifies the risks and the opportunities for the SHIELD solution. In the last part, the final per-partner exploitation plans, in addition to joint exploitation plans and results, are illustrated.

Compared to its first release (D6.3), this document provides the following updates:

- A detailed techno-economic analysis (Chap .3)
- Joint exploitation plans (Sec. 4.2)
- Identification of the SHIELD final results and owners (Sec. 4.1)
- Updates to the market analysis (Chap.2) and individual exploitation plans (Sec. 4.3)

2. MARKET ANALYSIS

2.1. Evolution of the market

Growth in worldwide cloud-based security services is expected to remain strong over the years to come, being greater than this of the total information security market[1]. Gartner estimates the cloud-based security services market will reach close to $9 billion by 2020.

Table 1. Worldwide Cloud-Based Security Services ($M) [1]

Segment	2016	2017	2018	2019	2020
Secure email gateway	654.9	702.7	752.3	811.5	873.2
Secure web gateway	635.9	707.8	786.0	873.2	970.8
IAM, IDaaS, user authentication	1,650.0	2,100.0	2,550.0	3,000.0	3,421.8
Remote vulnerability assessment	220.5	250.0	280.0	310.0	340.0
SIEM	286.8	359.0	430.0	512.1	606.7
Application security testing	341.0	397.3	455.5	514.0	571.1
Other cloud-based security services	1,051.0	1,334.0	1,609.0	1,788.0	2,140.0
Total Market	**4,840.1**	**5,850.8**	**6,862.9**	**7,808.8**	**8,923.6**

The penetration testing market is estimated to grow from USD 594.7 Million in 2016 to USD 1,724.3 Million by 2021, at a Compound Annual Growth Rate (CAGR) of 23.7%. The major forces driving the penetration testing market are the need for protection from various cyber-attacks and increasing number of mobile users and applications. The penetration testing market is growing rapidly because of the growing security needs of Internet of Things (IoT) and Bring Your Own Device (BYOD) trends and increased deployment of web & cloud-based business applications according to MarketsandMarkets[2].

According to IDC, public IT cloud services have an annual growth rate (CAGR) of 23.5%. By 2017, Software-as-a-Service remains the largest public IT services category, capturing 59.7% of revenues in 2017. PaaS and IaaS are expected to be the fastest growing categories (CAGRs of 29.7% and 27.2%).”

Also, if we focus the market trends in the Communication Service Provider (CSP) players and in the type of market offers, there is an increasing expansion in the service capacity. It started

[1] http://www.gartner.com/newsroom/id/3744617
[2] http://www.marketsandmarkets.com/PressReleases/penetration-testing.asp

with legacy Security products silos (Web or email security, IDS/IPS, Firewalls, Anti-malware products, etc.). Now, the market is oriented to Managed Security Service Providers (MSSP), where several CSPs are already offering this service (On premises or Cloud-based) that combines several of previous products, through a service bundle, including the management of the service. The next evolutionary step in the market will be to offer End-to-end Security Solutions. Gartner [3] predicts that this category, should be seen in the market in the next 2-5 years and will include consulting and professional services, management and intelligent analysis (Artificial intelligence) with strong focus in cybersecurity capabilities. It is clear that a service based on the SHIELD framework is well positioned to cover these CSP needs.

A more detailed requirements list of what should be expected in the market according to Ovum [4] and Forrester [5] should include:

- A shift from protecting the network to strategically ***protecting the business,*** including new capabilities: Consulting, analytics, data science, threat hunting, incident response, and remediation.
- Coverage of the new business opportunity: ***autonomic cyberhealth***. This involves integrating, orchestrating, and automating customers' existing security toolsets and/or helping them deploy predefined integrated security architectures.
- Investment focuses on ***prevention and detection vs mitigation*** through network monitoring, WAF, advanced threat detection, security analytics and DDoS.
- ***Augmented technology*** (well-trained machine algorithms by security experts) to cover lack of skilled technical staff.

New available data from Gartner in 2018 confirms the trends in security market[3], where there will be an increase in security investments by 40 percent, partially caused by GDPR and privacy concerns related to the companies' digital transformation.

Table 2 highlights the segments where SHIELD can leverage this opportunity:

Table 2. Worldwide Security Spending in Segments covered by SHIELD ($M) [2]

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237

[3] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

2.2. Possible competitors

This subsection provides an overview of products and services (in alphabetic order) which share specific features with SHIELD, and which already exist on the market. The overview is focused on Security Information and Event Management (SIEM) products, Security-as-a-Service and SDN/NFV products, including their main features and deployment options. Specifically, SIEM products are focused on providing visibility with respect to network and application conditions, thus allowing effective management of a cybersecurity incident. A multitude of SIEM products are offered as standalone appliances to be set up in the clients' data centers. The current trend of Security-as-a-Service pushes SIEM away from the appliance model to the cloud domain. The SIEM end user can thus purchase the required services without investing in further infrastructure.

Gartner[4] has also defined the integrated threat intelligence and response capabilities in a single flow, as SOAR (Security Orchestration, Automation and Response). According to Gartner, the share of organizations with security teams larger than five people will turn to integrated SOAR frameworks rather than individual products, for orchestration and automation. Gartner states that "most of the drivers have existed for as long as enterprise and government SOCs have existed — for decades, not years. However, SOAR tools only appeared in mid-2010s" and estimates that the market share for SOAR will rise from 1% to 15% by 2020. It also states that "as the security skills shortage persists, alert numbers and attack vectors grow, and product proliferation continues, more complex organizations will consider SOAR solutions to unlock the full potential of both their analysts and security product suite". SOAR can therefore be considered as a SIEM platform that features advanced analytics, threat intelligence and remediation in a single workflow. Although a lot of products can boast a SOAR workflow, there are no known SDN/NFV enabled SOAR platforms at this date.

Virtual Network Service products include the deployment of security services as virtualized components. Services can be tailored to include DDoS protection, Next Generation Firewalls, and other security products. To this day, there does not exist a commercial and integrated solution offering both SOAR capabilities combined with SDN/NFV network services. In this respect, SHIELD manages to organically link advanced SIEM with virtual network services. Easy deployment of network services and integration with DARE's SIEM capabilities is expected to be a key innovation of SHIELD, filling specific cybersecurity needs in existing (e.g Threat Intelligence) or fast growing markets (e.g. MEC).

2.3. Product Comparison

In this section, the main features of the aforementioned competitive products have been accumulated, in order to form a set of capabilities that should be present in state-of-the-art solutions like SHIELD. Effort has been made to provide an overview of the most important features of the three dominant types of cybersecurity products, namely SIEM, SecaaS and NFV/SDN. These features are presented in Table 2, forming the comparison criteria between SHIELD and similar products. Each product type specialises in a particular domain of network

[4] Anton Chuvakin, Augusto Barros, "Preparing your security operations for Orchestration and Automation tools", Gartner, February 2018.

protection, fulfilling specific needs; thus SIEM systems generally focus on providing advanced monitoring and threat detection techniques along with sophisticated incident response, SecaaS systems are characterised by ease of deployment and support simplicity, and NFV/SDN solutions are capable of defining and deploying advanced threat mitigation, through virtualized security services. Since most of these systems also share some common traits, these are depicted as general/generic capabilities. The fulfilment of each one of the different capabilities-criteria is being presented in Table 3 for SHIELD as well as for all products described in D6.3.

Table 2. Listing of criteria for product comparison

Criteria / Capabilities	Description	Category
Real-Time Security Monitoring	Provision of monitoring data and events in real-time	SIEM capabilities
Advanced threat detection	Detection of advanced, zero-day threats using ML and statistical analysis	SIEM capabilities
Data & End User Monitoring/SUBA	Security User Behaviour Analytics	SIEM capabilities
Data and Application Monitoring	Inclusion of application data (e.g. logs), in addition to network traffic	SIEM capabilities
Network analysis and visibility (NAV)	Analysis of network activity, detection of anomalies, user activity tracking, inventory of the infrastructure	SIEM capabilities
Advanced Analytics	Support for sophisticated quantitative methods (such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization)	SIEM capabilities
Log Management & Reporting	Creation of customised logs, human-readable reports	SIEM capabilities
Business Context and Security Intelligence/ Rules-based correlation	Business context in the form of asset criticality, usage, connectivity and ownership, as well as information about a user's role, responsibility and (employment) status aid in evaluating and analysing the risk and potential impact of an incident.	SIEM capabilities
Incident Response and Management/ Built-in workflow and investigation	Incident response and workflow support, including a role-based case and incident management system that manually and automatically aggregates events.	SIEM capabilities
Big data infrastructure	Infrastructure for storage and analysis based on Big Data technologies	SIEM capabilities
Ability to leverage third party threat intelligence	Ability to integrate third-party services for analytics	SIEM capabilities
PCI-compliant log archival	Compliance with Payment Card Industry Data Security Standard	SIEM capabilities
Advanced threat mitigation/defence	Enforcement of security through: - Definition and application of policies and configurations to existing vNSFs or applications	NFV + SDN Capabilities

Criteria / Capabilities	Description	Category
	- Traffic redirection - Instantiation of new security functions	
Data export and sharing	Support for standard formats (e.g. STIX) or proprietary with IoC (indicators of compromise) information: Events, logs, samples, IP list	NFV + SDN Capabilities
Infrastructure and service attestation	Automatic verification of the integrity of the infrastructure and/or service	NFV + SDN Capabilities
Integration with NFVI & NFV MANO	Capacity to deploy services using virtualization technology and service function chaining , based on orchestration technology	NFV + SDN Capabilities
Deployment and Support Simplicity	Easiness in deployment, installation and operation	General capabilities
Recommendation policy engine	The ability -based on data analytics, rules correlation, and business context- to generate recommendation to apply to mitigate incidents	General capabilities
Open Source code and integration	Integration of open-source platforms; release of parts of the product as open source	General capabilities
Standards ETSI compliance	Compliance of the architecture to ETSI and other international standards	General capabilities
Open API and protocols	Openly documented -and, preferably, standards-based- API for data exchange	General capabilities
Integration of third-party vNSFs	Support of 3rd-party services and vNSFs to add monitoring or mitigation capabilities.	General capabilities
Data exfiltration detection	Detection of data exfiltration incidents	General capabilities
L4/L7 Firewall	Inclusion of components with L4/L7 firewall capabilities	General capabilities
DDoS protection	Detection and mitigation of (D)DoS incidents	General capabilities

Table 3. Product Comparison - Capabilities

Criteria / Capabilities	SHIELD	AlienVault USM	AlienVault OSSIM	ArcadiaData	BlackStratus SIEMStorm	BlackStratus LogStorm	BlackStratus CyberShark	Cisco Umbrella	EMC (RSA) NetWitness	EventTracker	FortiSIEM	Fortinet NGFW	IBM Qradar	LogRhythm	ManageEngine	RAD Vcpe	SolarWinds	Splunk	VSS Nuage Net	Exabeam	Sumo Logic
Real-Time Security Monitoring	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓		✓	✓	✓	✓	✓
Advanced threat detection	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓		✓	✓		✓	
Data & End User Monitoring/SUBA		✓	✓		✓		✓	✓	✓	✓	✓		✓	✓			✓	✓		✓	✓
Data and Application Monitoring /	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓
Network analysis and visibility (NAV)	✓	✓		✓				✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓
Advanced Analytics	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	
Log Management & Reporting		✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓			✓	✓	✓	✓	✓
Business Context and Security Intelligence/ Rules-based correlation					✓	✓	✓							✓			✓	✓	✓	✓	✓
Incident Response and Management/ Built-in	✓	✓	✓	✓	✓	✓	✓		✓	✓				✓			✓	✓	✓	✓	✓

Criteria / Capabilities	SHIELD	AlienVault USM	AlienVault OSSIM	ArcadiaData	BlackStratus SIEMStorm	BlackStratus LogStorm	BlackStratus CyberShark	Cisco Umbrella	EMC (RSA) NetWitness	EventTracker	FortiSIEM	Fortinet NGFW	IBM Qradar	LogRhythm	ManageEngine	RAD Vcpe	SolarWinds	Splunk	VSS Nuage Net	Exabeam	Sumo Logic
workflow and investigation																					
Big data infrastructure	✓			✓	✓	✓	✓		✓				✓	✓				✓	✓	✓	✓
Ability to leverage third party threat intelligence	✓	✓	✓							✓	✓		✓	✓			✓	✓			
PCI-compliant log archival		✓			✓	✓	✓			✓				✓			✓	✓	✓		
Advanced threat mitigation/defence	✓			✓							✓						✓		✓	✓	✓
Data export and sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓				✓		✓	✓
Infrastructure and service attestation	✓																				✓
Integration with NFVI & NFV MANO	✓															✓			✓		
Deployment and Support Simplicity	✓	✓		✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	
Recommendation policy engine	✓	✓	✓		✓	✓	✓							✓			✓	✓	✓	✓	
Open Source code and integration	✓		✓	✓										✓							
Standards ETSI compliance	✓															✓			✓		

Criteria / Capabilities	SHIELD	AlienVault USM	AlienVault OSSIM	ArcadiaData	BlackStratus SIEMStorm	BlackStratus LogStorm	BlackStratus CyberShark	Cisco Umbrella	EMC (RSA) NetWitness	EventTracker	FortiSIEM	Fortinet NGFW	IBM Qradar	LogRhythm	ManageEngine	RAD Vcpe	SolarWinds	Splunk	VSS Nuage Net	Exabeam	Sumo Logic
Open API and protocols	✓	✓	✓	✓				✓			✓				✓	✓			✓		
Integration of third-party vNSFs	✓										✓					✓			✓		
Data exfiltration detection	✓							✓	✓			✓	✓								✓
L4/L7 Firewall	✓							✓		✓		✓					✓		✓		
DDoS protection	✓							✓		✓							✓		✓	✓	

.

The above table (Table 3) has been updated since D6.3, to present a comprehensive capabilities comparison between SHIELD and other similar products that were described in D6.3 as of M29 of the project. Since the modern market comprises of competitors that offer a variety of different cybersecurity services (SIEM, SecaaS, SDN/NFV, etc.), it is obvious that a direct comparison of their main features is -in most cases- not applicable. However, the idea behind this comparison was to distinguish the most important functionalities of each category (Table 2), in order to extract a set of criteria that will be used to review SHIELD as a competitive "all-in-one" cybersecurity approach. Given the growing need for automation in threat detection, analysis and mitigation, the fulfilment of these criteria would render SHIELD a reliable solution for all types of organisations and ISPs.

As depicted in Table 3, the increasing number of vendors that have adopted non-traditional cybersecurity elements acknowledges the versatility of the SHIELD platform. Despite the addition of a number of competitors, the core capabilities of the platform, including centralized visibility, virtualisation of services (SecaaS), aggregated threat detection mechanisms, utilization of Big Data technologies for scalable processing of largely unstructured data and the leveraging of machine learning for anomaly detection and threat classification, are shared between SHIELD and the majority of the vendors, thus rendering it up-to-date with the existing trends in the cybersecurity landscape. In addition to including typical SIEM features like real-time monitoring and advanced threat detection, SHIELD is also adding novelties that are missing from the majority of competitive products, such as infrastructure attestation, and parallel advanced analytics offered by two cybersecurity engines. At the same time, SHIELD is based on open-source technologies thus allowing for the development, modification and integration of third-party services and for the exploitation of the engine's APIs and protocols. Overall, SHIELD seems to encapsulate all the innovative features of a successful cybersecurity product in accordance with today's standards and remains a valid solution of great market potential.

2.4. Barriers for SHIELD

SHIELD is a newcomer on a very competitive market, populated mostly by companies that offer integrated SIEM and NGFW service suites with the possibility of adding extra functionality as the deployment complexity increases. In order to enter this market, SHIELD has to overcome a few major hurdles that will be common to any newcomers.

The first major barrier to adoption is the trust on the vendor. As a newcomer to the market, SHIELD will struggle to become a recognized trusted service. On the other hand, other services that may or may not overlap functionality with SHIELD have well established names due to ongoing and long lasting marketing investments or due to well-known results in the case of open source projects. To counterbalance this, SHIELD vendors will likely need to operate with revenue losses while the system makes a reputation for itself, either via very aggressive pricing models or via free trials. Another, more feasible approach, is to offer SHIELD via a well-established telco (according to the Telecom Security Service/TSS business model, which has been identified as the most relevant one in D2.3). In this way, market entrance can leverage the trust on the telco (rather than on the vendor).

The second major barrier to adoption is vendor lock in. For an existing company, even if SHIELD may be a better option from a pure technical perspective, the adoption of a product that can integrate with existing SIEM or UTM platforms that are already in operation on the network

may seem as an advantage. The company will claim this will decrease the total cost of ownership as the cost of integration with existing systems and the cost of training personnel on the usage of the new tool will usually be lower if the tool integrates smoothly within the current solution ecosystem. To prevail, SHIELD must offer open, easy to integrate APIs, and potentially try to create value via the integration with third party management systems (although this is not part of the project). Such integrations would lower the perceived barrier, allowing decision makers to focus more on the innovative functional aspects of the solution.

A third barrier to adoption is the market positioning. SHIELD tries to leverage a set of technologies that are now emerging and are expected to become commonplace in a few years. Hence, the adoption of SHIELD cannot grow any faster than the adoption of the technologies on which it is based. Even if the base technologies are widely adopted, the SHIELD market cap will always be a fraction of the operators that are of the correct size to adopt a SHIELD solution and have the need for the adoption of an advanced security system that runs on a trusted platform. The only way to vanquish this barrier is through marketing and advocacy. Getting the decision maker to understand the advantages of SHIELD over its competition, especially if the decision maker does not have technical skills which will require a multi-pronged marketing campaign, focused both on the technical advantages and on the business advantages according to the target audiences.

A last barrier worth mentioning is the usability. While on the early stages of researching a product, one of the first things that an operator will do right after reading the datasheet is to look for screenshots and videos showing how to use the platform. During this stage, a bad UI or a complex iteration will most likely relegate SHIELD to the back of the line of the products under review, and it may be hard to recover from that given the barriers described above. The careful and timely dissemination of materials showing the user iteration and experience helps to overcome this barrier. These materials should target both technical and non-technical audience. If the platform looks and feels pleasant to use, the likelihood of the potential client taking the next step towards the adoption should be a lot higher, allowing more opportunities for a pre-sales team to close the deal.

In order to maximise its adoption chances, SHIELD has to overcome a few major barriers that have been identified in this document. The aim should be that the selected business model should overcome most of the barriers by addressing the lock and trust in the vendor, leveraging the trust in the Operator.

2.5. SWOT and Business Modelling Analysis

Figure 1 below illustrated the initial SWOT analysis which had been available at the early stage of the project.

Figure 1. SWOT Analysis (initial approach)

Initial conclusions show that cost reduction or a well-defined price model will cover a wide range of different types of client demands opportunities. The first stage is to decide the client type and the type of service. Therefore, a specific business model definition is needed.

Today, there is a strong fragmented market, as it is shown in the variety of competitors in different areas (see section 2.2, 2.3). The prediction on how the market will evolve (see section **Error! Reference source not found.**) shows a clear threat in the SWOT: consolidation in few big players with end to end services. SHIELD can leverage this opportunity if a robust technology framework output is created.

Finally, Privacy is seen as a risk caused by the absence of clear regulatory framework in the security area. The GDPR, for example, is at the same time a threat, because requires strong protection of personal data, and also an opportunity of SHIELD to help protecting the privacy via early detection of cybersecurity incidents such as data exfiltration.

Previous sections with insights from the market evolution to the market competitor, allows us to elaborate a technical SWOT (Figure 2), in this case oriented to Managed Security Services Providers (MSSP).

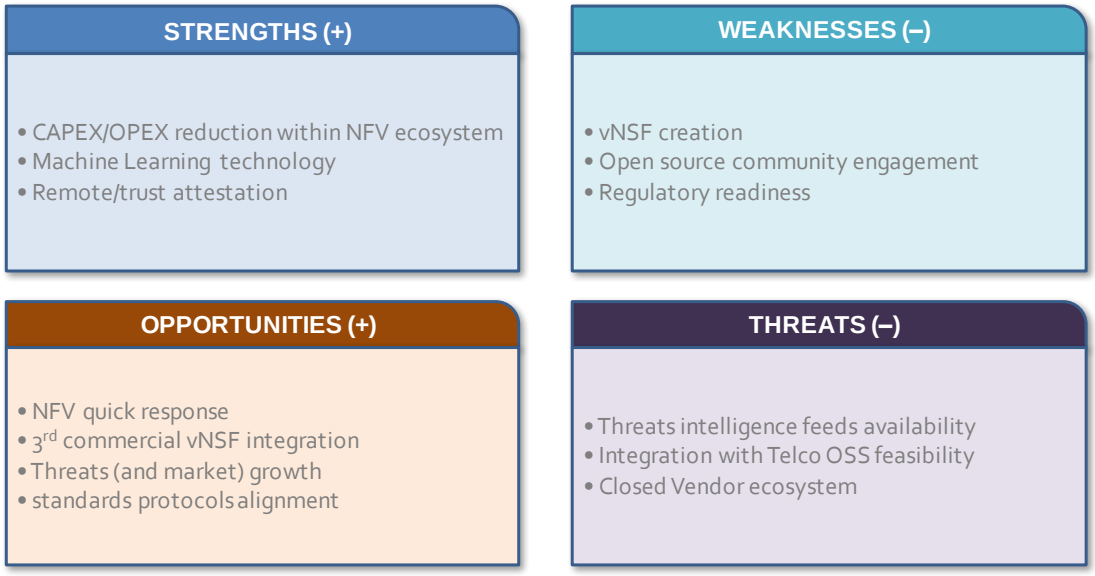


Figure 2. Technical SWOT Analysis for SHIELD-based Managed Security Service (updated)

The conclusions that can be extracted from this exercise are:

NFV must be enforced as a key technology for MSS. Adopting NFV technology jointly with open standards (ETSI NFV) and leveraging open-source platforms such as Open Source MANO, can be seen as a clear competitive advantage.

In open NFV-based solutions such as SHIELD, there is a clear risk in the lack of security offers if there is no involvement of vNSF security vendors (vNSF developers). This evolution is already present in some commercial solutions (e.g. RAD and Nokia), yet the strong market growth is expected in the next years. Therefore, the long-term solution, once the framework is functional, should involve relevant vNSF vendors.

Real time monitoring, analytics, threat intelligence and advanced mitigation support are part of the commercial offerings. Lack of cyber threats feeds in order to better shape the rules and/or train Machine Learning algorithms, is an issue that should be faced.

Remote attestation today is a research domain, meanwhile commercial solutions are focused more on vNSFs image integrity. Bringing mechanisms such as remote attestation from the research field to a commercial NFV solution is a clear differentiating factor to be prioritized.

Detailed business model opportunities were studied and presented in D2.3, using Figure 2 technical SWOT as a baseline. As a result, the ***Telecom Security Service*** (TSS) business model proposes a network-based solution that combines the availability of a Telco network operator, including NFV technology, with the SHIELD Framework to deploy a MSS (Managed Security Service). Figure 3 summarizes the business model and the canvas elaborated in D2.3.

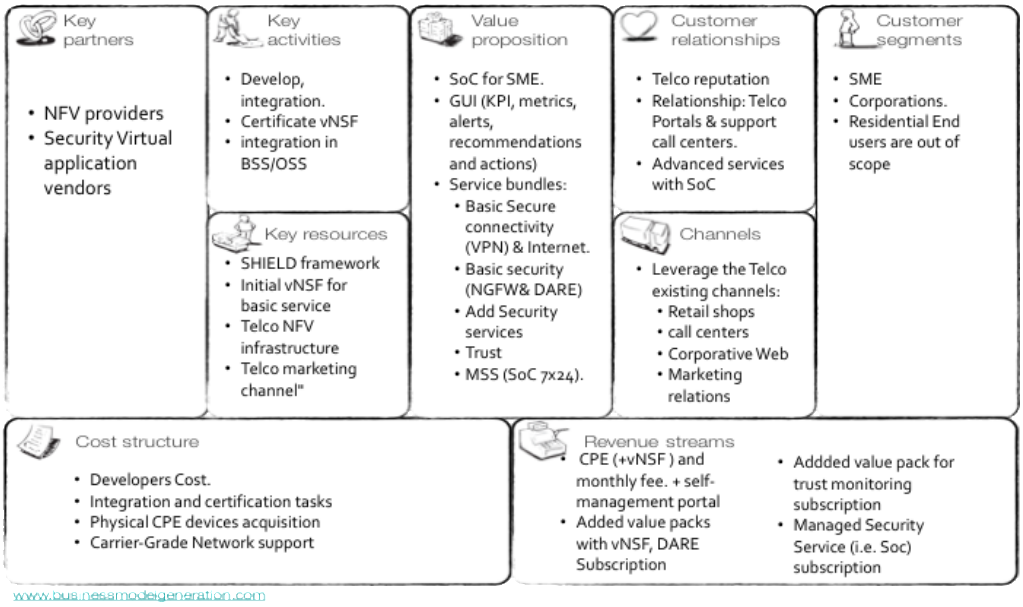


Figure 3 TSS Business Model Canvas

Also, one additional potential service was identified, the ***Trust Monitoring as a Service*** (TMaaS). This business model proposes an infrastructure verification solution offered as-a-Service. The solution is based on trust attestation using Trusted Platform Modules and related Trusted Computing technologies. Figure 4 summarizes the business model and the canvas elaborated in D2.3.

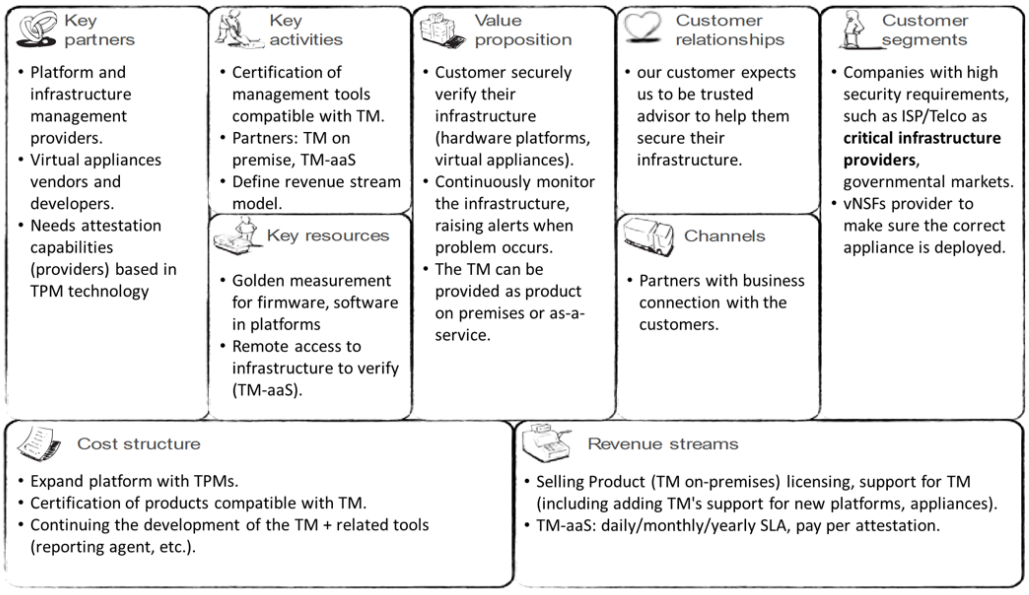


Figure 4 TM-aaS Business Model Canvas

3. TECHNO ECONOMIC ANALYSIS

3.1. Techno-economic Framework

The objective of the techno-economic analysis is to make an estimation of the associated capital expenditure (CAPEX) investments costs, revenues, and operational expenditures (OPEX) over a selected period of time. The final aim is to estimate the future cash flows that are calculated by taking into account the CAPEX and OPEX, as well as the revenue streams; the hope being that the cash flows will become positive within the selected period of time.

The techno-economic methodology is based on a bottom-up analysis of discounted cash flows for network deployment, operation and maintenance. The techno-economic tool is based on the tool developed within a series of techno-economic projects, namely TONIC[5], ECOSYS[6], TITAN and it has been used in several related network evaluation studies for mobile and fixed networks.

The technical and economic analysis has to consider the objectives to be reached (in terms of service demand, sales or target customers), the network architecture and requested resources, the planned expenses, and other costs that are not directly assigned to the activity.

Input elements related to the cash flow analysis are:

- Revenues
- Investments / CAPEX (Capital Expenditures)
- OPEX (Operational Expenditures)

CAPEX is defined as those expenditures associated with the implementation or extension of assets (like network infrastructure), subject to depreciation over the economic life of a project. CAPEX is indispensable for new service provisioning or improvement of existing services, or for enhancement of the company business. CAPEX analysis is generally based on the physical and logical resource requirements

OPEX is defined as those expenditures necessary for running the business or the equipment, indispensable to keep the services active and running. These expenses are not intended to extend the functionalities of the fixed asset and are not subject to depreciation. Once made, these expenses have no residual value.

At the overall level, OPEX is defined in this work as all those cost elements in the cash flow analysis that are not CAPEX. In reality, the border between CAPEX and OPEX is not always so clearly defined. Some expenses, like those related to software, are at the border between CAPEX and OPEX, because there are aspects here that are related to each other.

All purchases of hardware and software systems is defined as CAPEX, but the operation and maintenance of these systems, as well as related manpower costs and license costs are OPEX.

The core part of the model are the cost figures for different network or IT components. These data are collected regularly, and being updated by getting information from

[5] http://cordis.europa.eu/project/rcn/53630_en.html
[6] https://www.celticplus.eu/project-ecosys/

telecommunication providers, vendors, and benchmarks from the telecoms market and the project.

The data contains the initial prices for commercial networks components, and a projection for their future production volume. The cost evolution of the different components derives from the cost in a given reference year and a set of parameters which characterises each component.

The length of the study period is always adapted to the specific case under investigation. For the case of SHIELD, and considering the time a network or a service needs to reach market maturity in order to pay back investments, an eight commercial year period is considered reasonable, plus one for the preparation of the products.

As a first step, the services are defined along with their requirements, with the next step containing the analysis and description of the network architecture and all the necessary elements that are needed in order to provide the defined set of services.

The future market penetration of these services and the tariffs associated with them are used for the construction of the market evolution model. By combining market penetration and tariff evolution, one can calculate the received revenues for each service.

To calculate the expenditures, the selected topology and the dimensioning rules for the NFV components and the IT resources to be used are required. The output of the so-called "architecture scenario definition" is a shopping list that contains all the required elements (like project network planning).

To calculate the number of network components required throughout the study period, demand forecasting is carried out using existing methodologies and market data as shown in the following section.

CAPEX is then calculated by combining the required numbers of components and their price for each year. A price evolution is calculated for all network components using mainly the fixed curve model.

OPEX are calculated as a fixed percentage of the total investments in network elements plus a maintenance cost in addition to the overall CAPEX and OPEX cost.

By entering the data into the financial model, the model calculates the revenues, investments, cash flows and profits (or other financial results) of the study network architectures for each year of a project's study period. In the final evaluation of the techno-economic model, critical indexes are calculated in order to decide about the profitability of the investment.

The first output is the investment cost of the project of SHIELD deployment. Because the methodology studies scenarios, the investments are usually spread over the study period. To get a single figure of merit for the total investment, the future investments are discounted to the start of the study period using the conventional discounting formula. The total discounted investment cost is usually called First Installed Cost.

The current implementation of the methodology allows the investments to be analysed based on physical location of the cost components in the network (by hierarchical network level).

Discounted Cash Flow (DCF) analysis takes into account the time value of money and the risks of investing in a project. Towards this end, cash flows for future investments are estimated and discounted in order to calculate the Present Value (PV). The main advantages of DCF analysis

are that it is a simple quantitative method to implement, is widely accepted, and provides clear and consistent metrics for all kinds of projects.

Some common metrics that are used to judge the cash flows are the following:

- The Net Present Value (NPV) is the present value of the future cash flows (revenues less costs), discounted using a factor that resembles the time-value of money. If the NPV is positive, the project is judged profitable. The Net Present Value gives a single figure of merit for a project. In addition, we can calculate the Salvage value (rest value) as the estimated amount that an asset is worth at the end of its useful life.
- The Internal Rate of Return (IRR) is calculated as the discount factor that results in a zero-NPV. A higher IRR means higher profitability and better return on investment. IRR is a useful metric in the case where the scenarios to be compared are of different size and scope, for example if the size of the networks is different. In these cases, the scenarios cannot be easily compared using Net Present Values, but Internal Rate of Return gives a good indication of the relative profitability levels of the scenarios.
- The Payback Period is the number of years that are required to recover the initial invested money. In an investment scenario where most of the expenditure happens in the beginning of the study period, the Payback Period gives a good indication of the efficiency of the investment. If the scenario is more complex, for example if there are several technology steps in an upgrade situation, it is not possible to define a single Payback Period.
- A typical Cash Balance (or accumulated cash flow) curve for a Greenfield network deployment scenario initially goes deeply down into the negative side because of the high initial investments. If the scenario is profitable, the cash flow turns positive fairly soon and the Cash Balance curve starts to rise. The lowest point in the Cash Balance curve gives the amount of funding required for the project. The point in time when the Cash Balance turns positive gives the Payback Period for the project.

The results presented in this deliverable will focus mainly on Net Present Value (NPV) and Cash Balance. In the evaluation of investment scenarios there can be several points of view. Depending on the complexity of the scenario various commonly used indicators, like Payback Period, NPV or IRR, can give differing results in comparisons. Because of this, it is often necessary to use several figures of merit for the studies to get a thorough understanding of the economic issues related to each scenario. In most of the cases these evaluations have some less known inputs. In these cases, it is advisable to apply a sensitivity analysis and/or risk assessment methodologies to these inputs using multiple figures of merit as indicators.

The derived results concern a set of scenarios with specific parameters values. However, in the case of fluctuations in the values of critical parameters, a sensitivity analysis should be performed. The parameters are varied by a selected percentage (%) in order to assess their impact on the key performance indicators of the project. Note that a sensitivity analysis can be performed for all parameters that affect both the model and the key financial indicators.

The risk analysis is based on the use of Monte Carlo simulation. The underlying variables in a business case, e.g. prices, future market shares, cost evolution and demand are inherently uncertain. This means that the decision maker must model the uncertainty of relevant variables in order to see the impact on the derived result. Uncertainty about a situation can often indicate risk, which is the possibility of loss, damage or any other undesirable event.

The difference between a traditional "plain" sensitivity analysis and a risk analysis based on Monte Carlo simulation is that the former only tells you what is possible; not what is probable! In traditional sensitivity analyses, a number of variables are selected for the study and varied one at a time to see the impact on the main result. Often "what if" scenarios are constructed with different combinations of worst-case, moderate, and best-case values of each of the variables – a very time-consuming process. Monte Carlo simulation, however, makes it possible not only to assign probabilities to each variable (we know that some variables are more uncertain than others) but also to update all the selected variables automatically and simultaneously. Random numbers according to the selected distributions are generated for each of the selected variables for the risk analysis. The simulation therefore calculates a large number (maybe thousands; the number of simulation trials is specified by the user) of "what if" scenarios. Equally important: the simulation keeps track of the calculations by measuring the impact on the result from the changes in each of the variables.

The type of distribution to choose for the variables under investigation is based on its conditions. For instance, it can be a variable that can never be outside a given interval, e.g. never be negative.

After having run a simulation of, e.g. 1000 trials, 1000 possible outcomes have been created compared to the single value obtained in the deterministic model. In addition to the statistics (mean value, percentiles and standard deviation) on the result variable(s), the input variables are ranked with respect to their impact on the outputs. The measure is either the contribution to the variance of the output variable(s) or the rank correlation. Some variables may show very little significance after all and could therefore be removed in future simulations. This will increase clarity as well as reduce the time it takes to complete a simulation.

Most often, probability distributions are defined by a mean value and a standard deviation. However, these parameters are not very intuitive. It is more intuitive to describe a variable by a default value/most expected value and by a confidence interval. A confidence interval of 90% means that there is a probability of 90% that the variable will take a value within the specified interval in a trial of a simulation.

In order to identify the impact of variations in key input parameters and following the initial results, this study includes a sensitivity and risk analysis with respect to parameters such as overall penetration, equipment costs, OPEX, traffic, and average revenue per user (ARPU).

3.2. Forecast and traffic estimations

3.2.1. Subscribers Forecast and Market Definition

An estimation of the market dynamics for the SHIELD TSS offering can be derived using observations from the cloud computing market. The cloud market is currently at an early stage even if the new indications from Eurostat show that the market has a great potential among the SMEs

Some highlights from the Use of cloud computing [10]:

- 26 % of EU enterprises used cloud computing in 2018, mostly for hosting their e-mail systems and storing files in an electronic format.

- 55 % of those firms used advanced cloud services relating to financial and accounting software applications, customer relationship management or to the use of computing power to run business applications.
- In 2018, a greater number of firms preferred public cloud servers (18 %) than private cloud servers (11 %), i.e. infrastructure for their exclusive use.
- Compared with 2014, the use of cloud computing increased particularly in large enterprises (+21 percentage points).

Cloud computing services are being used by more than one out of four enterprises in the EU and 12% of enterprises reported analysing big data.

Service providers can deliver cloud computing services with all the above characteristics in two main ways: via public cloud servers (18 % of enterprises) or private cloud servers (11 % of enterprises). The latter, by definition, involves a single-tenant environment where the hardware, storage and network are set aside for a single enterprise. Consequently, the infrastructure guarantees high levels of security, as the service provider's other clients cannot access the same resources. Some 11 % of SMEs and 31 % of large enterprises reported using private cloud (see Figure 5).

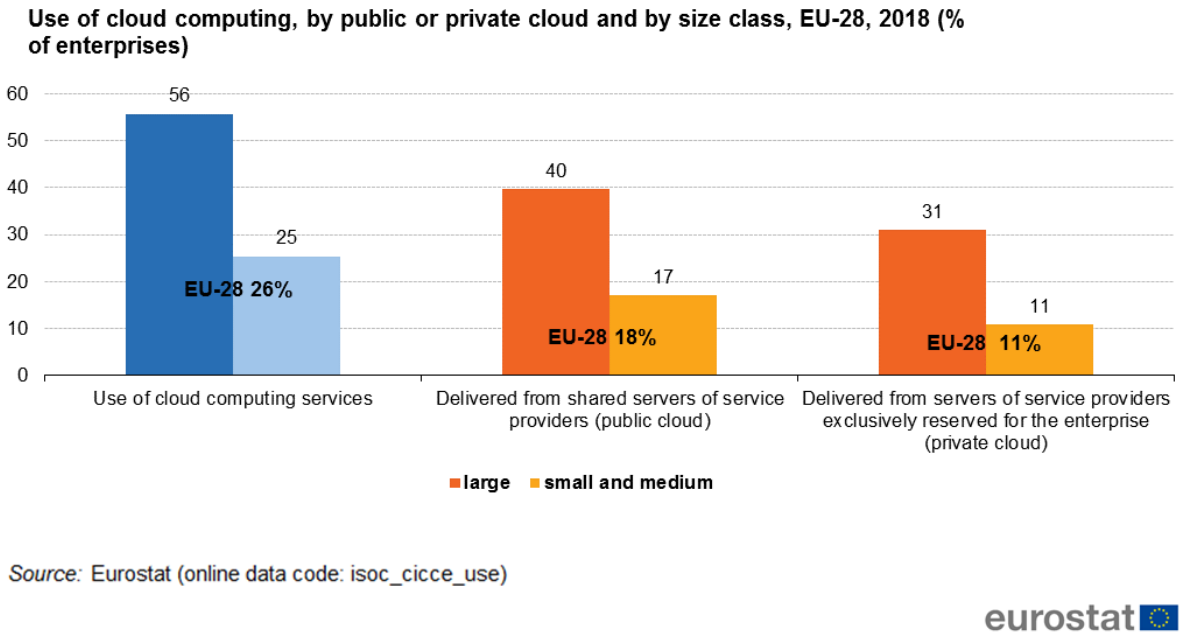


Figure 5. Use of Cloud services (source Eurostat [10])

Another market to be observed is the one related to information security. It is worth mention that the revenues of the biggest companies in the sector have been quadrupled in the last ten years (Fortinet, Juniper, Cisco, Palo Alto, CheckPoint, Symantec, IBM etc).

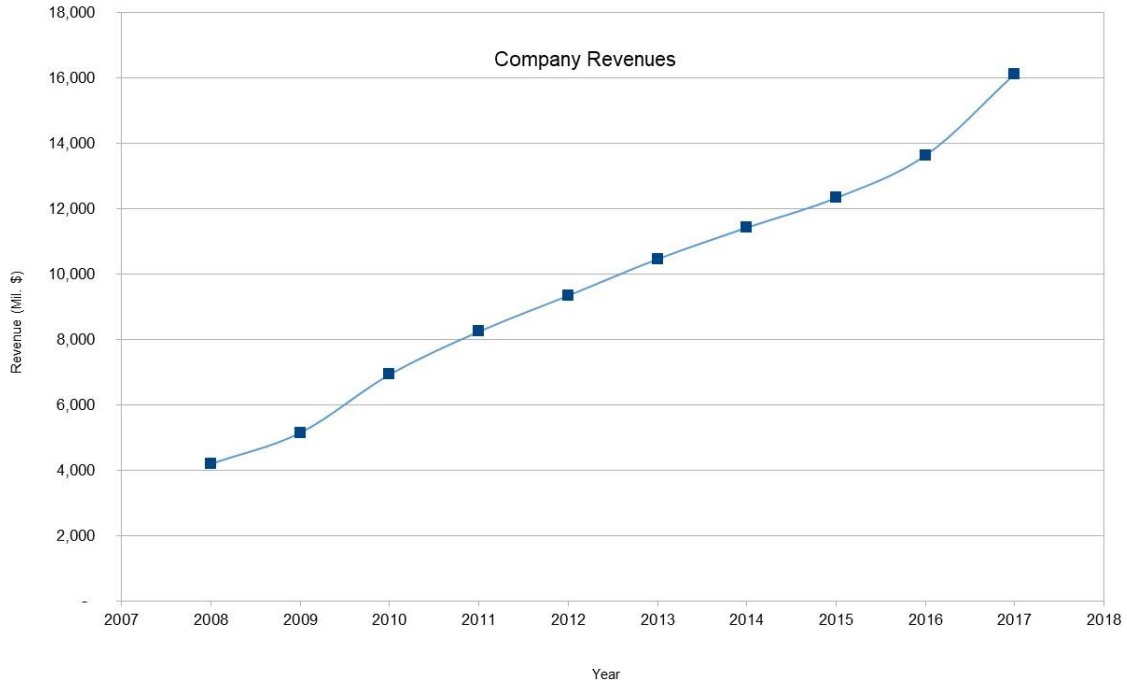


Figure 6. Company revenues in the last decade[7]

Based on these market dynamics, we can attempt an approximation of the market demand for Managed Telecom Security Services (TSS), as the ones provided using the SHIELD framework. The demand is based on the data of NGA (Next Generation Access) evolution and subscriptions of SMEs in EU for the years 2009 to 2018 in Europe [12] as an innovative service "S-curve" cumulative demand adoption model. Three diffusion models were employed for fitting, Logistic[8], Gompertz and Tonic [13]. Although the differences between Tonic and Gompertz were not significant (less than 0.5% on a yearly basis), Tonic model showed that it can fit the aforementioned data with lower error values compared to the other two diffusion models. The Tonic model was developed within the IST-TONIC project and provided reasonably accurate fitting over historical data related to high-technology products.

Three curves of demand were calculated, a pessimistic one based on countries with low NGA demand, an optimistic based on countries with high NGA demand and a baseline of medium demand based on countries close to the EU average NGA demand (Figure 7). The results presented will be based only in the medium demand case. The market penetration is expected reach to 10% of SMEs in 2035 (expected subscribers).

[7] Source inCITES

[8] https://en.wikipedia.org/wiki/Logistic_function

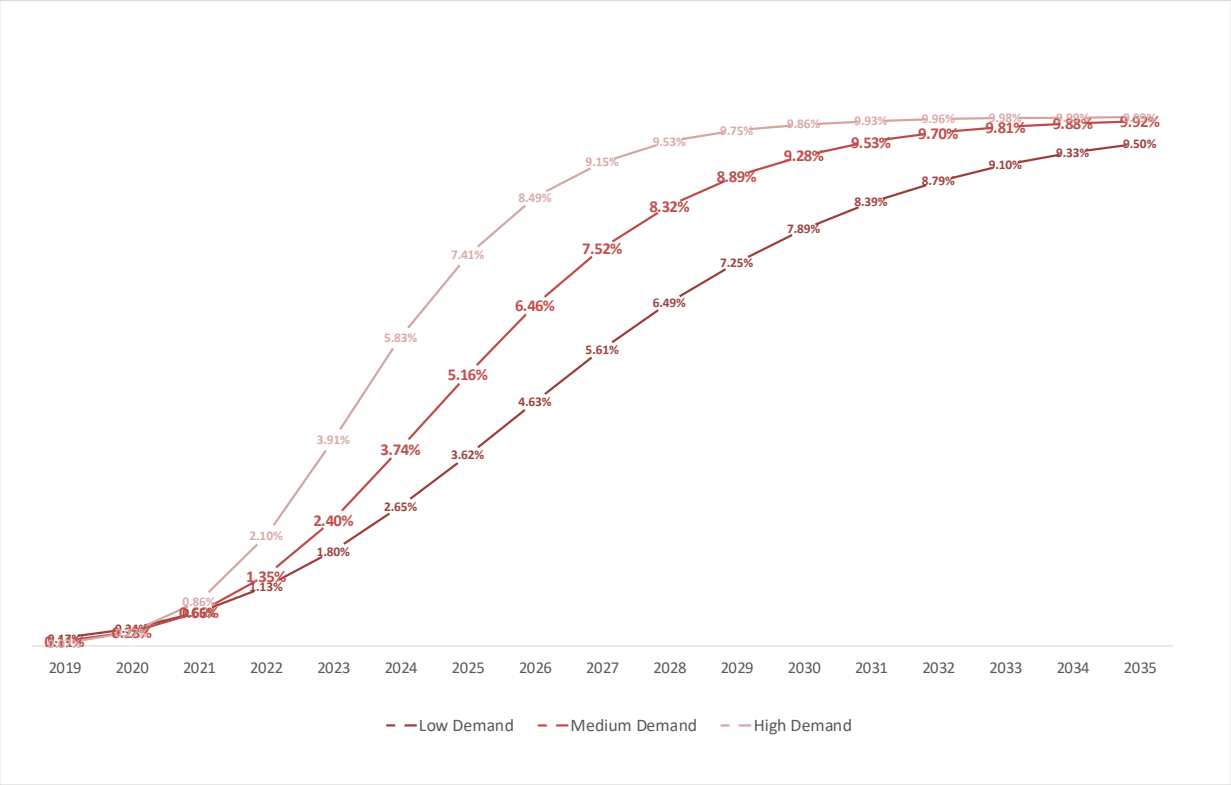


Figure 7. Forecast of Security Services (S- Curve)

Most of the SMEs (60%) already have security solutions installed but only 13% of companies have the service with an Operator which is quite a challenge for our case in the TSS model[9]. SHIELD could be an opportunity to attract more customers from traditional Business Solutions that have been already in place to TSS, Telcos will leverage their customer relations to offer a SHIELD based security service. Residential users are not in the main focus. In addition to that, Telco's reputation and brand image should be used to attract clients. Once a client is captured, in case of SMEs, a basic relationship will be established through web portals and support call centers. On the contrary, for clients demanding advanced services, personalized marketing can be used.

Assuming a nation-wide targeting by a national telco, our total market segment, according to Eurostat, is around 650,000 SMEs in a large European country (Like Spain[10]), or 500,000 in France. UK goes around 800,000 and Germany up to 212,000 in the total market (all SMEs). German SMEs are comparatively large: it is true that the SME sector is dominated by micro-enterprises with fewer than 10 employees, but 17 percent of SMEs are small and medium-sized enterprises in Germany (with 10–49 or 50-249 employees) – in the EU-27 average, only 8 percent of SMEs have more than 10 employees[11]. In our case we consider our target market to be the SMEs with a headcount between 10 and 250 employees. This number is approximately 250,000 SMEs in a country like Spain.

This is a crucial parameter since the expansion to a market segment (SMEs with less than 10 employees) could either fund or kill the business case.

[9] Analysis report
[10] From 0 to 1 person employed in the transport sector has not been included
[11] The German Mittelstand: Facts and figures about German SMEs

The size of the country is indicative since a NFV solution could successfully be deployed in a Pan European Level. In our study we consider as possible clients the SMEs with more than 10 employees. The SMEs percentage with "maximum contracted download speed of 100 Mb/s" in a Large Country according to Eurostat it is around 30% of the overall SMEs number and will grow in the next years[12]. As a result, the total number of SMEs targeting into our services is illustrated in the next plot assuming a 33% Market Share for our TSS operator.

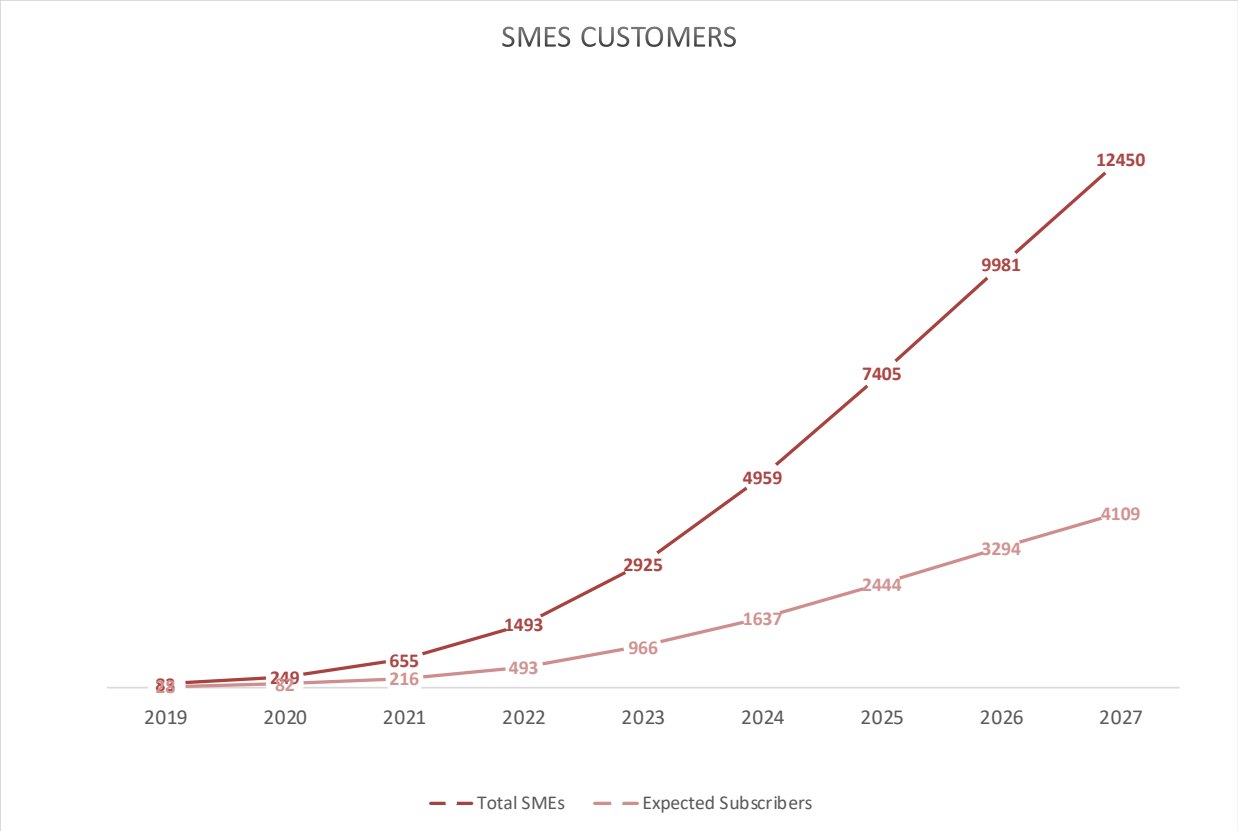


Figure 8. Total number of SMEs (customers of SHIELD Security Services)

One of the outcomes of the study presented in the next chapters is the minimum saturation level needed in order to have a profitable case study. In addition, the inclusion of clients with lower broadband connection will be investigated with very Small SMEs being excluded. Additionally, we assumed a tariff digression of 3%.

3.2.2. Traffic Calculations

The usage scenario estimates that traffic is coming from SHIELD's solution clients (usually SMEs) as described in the previous paragraphs. In order to dimension the traffic profile per expected client, a mean traffic value (in Mbps) has been used per 100 Mbps connection. In most of the public NGA models used for regulated cost oriented services, the average traffic per broadband subscribers is less than 5 Mbps in the busy hour. In some countries, the average traffic goes down to 2 Mbps. In our estimation, an average value of 5 Mbps has been used (Fiber-Connected

[12] https://ec.europa.eu/eurostat/data/database?node_code=isoc_ci_it_en2#

users generate more traffic compared to other sources of broadband[13]). The majority of the 100 Mbps connections is likely to be Fiber based in the near future and the total traffic will increase by 12% per year in a conservative forecast. In this context, a sensitivity Risk analysis has been performed, taking into account various scenarios for per-client traffic increase. This calculation is relevant to the services using vNSFs in the data plane, which process the total client traffic. For the relevant services using DARE, it processes only traffic information (e.g. flow data). This is only a fraction of the total traffic. For example, according to several sources Netflow bandwidth estimation is around 1-1.5% of the throughput[14].

Our initial assumption includes all SMEs with a specific broadband connection (employee count: 10-19 Small, 20-49 Medium and 50-249 Large). Security services could be offered to small companies and managed security to medium and large companies. As our previous market study shows (D2.3, D6.3), SHIELD has more exploitation potential in Medium Companies with possibilities to spread it to small companies in the near future. So we included in our calculations the traffic and we will investigated the impact of including micro SMEs to our study (additional Client segment).

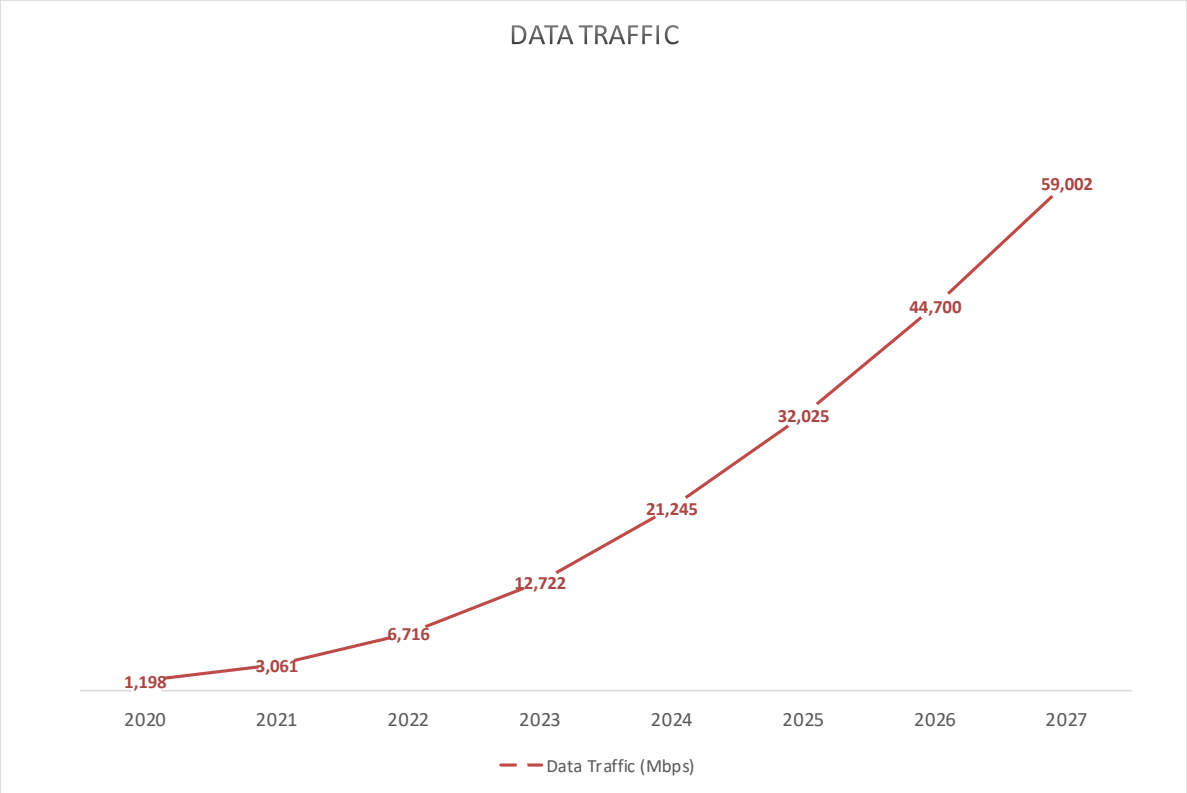


Figure 9. Total Generated Traffic from SMEs (clients)

[13] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc529314190

[14] Available online https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_presentation0900aecd80311f60.pdf

3.2.3. Financial Assumptions

A study period of nine years and a discount factor of 12% are used in the scenarios, while the taxation percentage rate is assumed to be 20%. In addition, a straight line depreciation was used based on the lifetime of assets.

Table 4 Financial Assumptions

Parameters	Value
Study Period	9 years
Starting Year (Implementation)	2019
Starting Year Operation	2020
End Year	2027
Discount Factor (WACC - Weighted Average Cost of Capital)	12%
Tax Percentage	20%

3.2.4. Service Definition and Revenue estimations

According to our use cases definition and the work carried out in the demos and pilots trails a set of services have been selected. These services are offered as part of the TSS bundle from a TSS operator in collaboration with SMEs, like NFV technology providers, vNSF developers and Data Analytics Providers.

Service component 1: Security Analytics

This offers the capability to centrally analyse the clients' traffic and achieve detection and classification of security incidents. It requires a full DARE installation, as well as the traffic collector modules.

Service component 2: Virtual Network Security Services (vNSFs)

This offers virtualised security appliances as vNSFs. This requires the establishment of the vNSF ecosystem, as well as the service catalogue and MANO components.

Service component 3: Attestation

This offers the capability securely and continuously monitor the infrastructure and services, raising alerts upon integrity check failures. This requires the installation of the Trust Monitor (TM) and its agents in virtual and physical assets.

For the purpose of this TE model, the following service packages are considered.

Table 5 SHIELD Services Offered

Sx	Description	Security Analytics	vNSFs	Attestation
S1	DARE Security Analytics	✓		
S2	vNSFs+DARE,	✓	✓	
S3	vNSFs+attestation		✓	✓
S4	vNSFs+DARE+attestation (full SHIELD)	✓	✓	✓

Only the revenues coming from pre-defined 4 services are considered in this analysis. There are additional potential revenues from the verticals applications, but these are not modelled specifically.

The assumptions concerning the monthly ARPU for the different types of service profiles are presented in Table 6; with these prices declining at a rate of 3% per year.

We note that these values indicate the additional incremental revenue that the TSS can get from BB clients over its network (i.e. this revenue is on top the broadband connection fee). These revenues could be share with other SMEs participating in the TSS business model. Another approach used in other business implementation (like 5G networks) is to interpret the incremental ARPU as the premium that users are willing to pay in order to get the improved security provided by managed security services.

One of the most important part of the study is the cost-oriented approach used with the completion of the TE model in order to clearly define the cost structure among the offered products. In our TE model, the actual cost created by each service is calculated in a Bottom up approach within the cost causality principle. So, the actual cost per service for the forecasted number of clients is calculated and inserted in the APRU as a difference in tariff between the services in order to charge equally the blend of services. The table below shows the target ARPU per service package and the envisioned demand per packet.

Table 6 ARPU per Service package

Sx	Service Description	ARPU (Tariff) / month	Demand per Packet	Pricing Structure of the basic tariff (Gradient)
S1	NSFs+DARE+attestation (full SHIELD)	40.00 €	50%	100%
S2	vNSFs+attestation	28.00 €	20%	70%
S3	vNSFs+DARE	32.00 €	20%	80%
S4	DARE Security Analytics	20.00 €	10%	50%

The calculation of the revenues is the outcome of the multiplication of the expected number of users with the average revenue per package (Sx). It is normal for the Operators to have a blend of services from different tariff gradients.

3.3. Scenario Definition - Deployment - Architecture

The SHIELD architecture as defined in the deliverables D3.2, D4.2, D3.3 and D4.3, will be used in this study. What follows is a general deployment configuration for the adoption of TSS business model in a Telecom Operator as used for the scope of the TE analysis; more details are provided in the previous deliverables or in the description of the use cases.

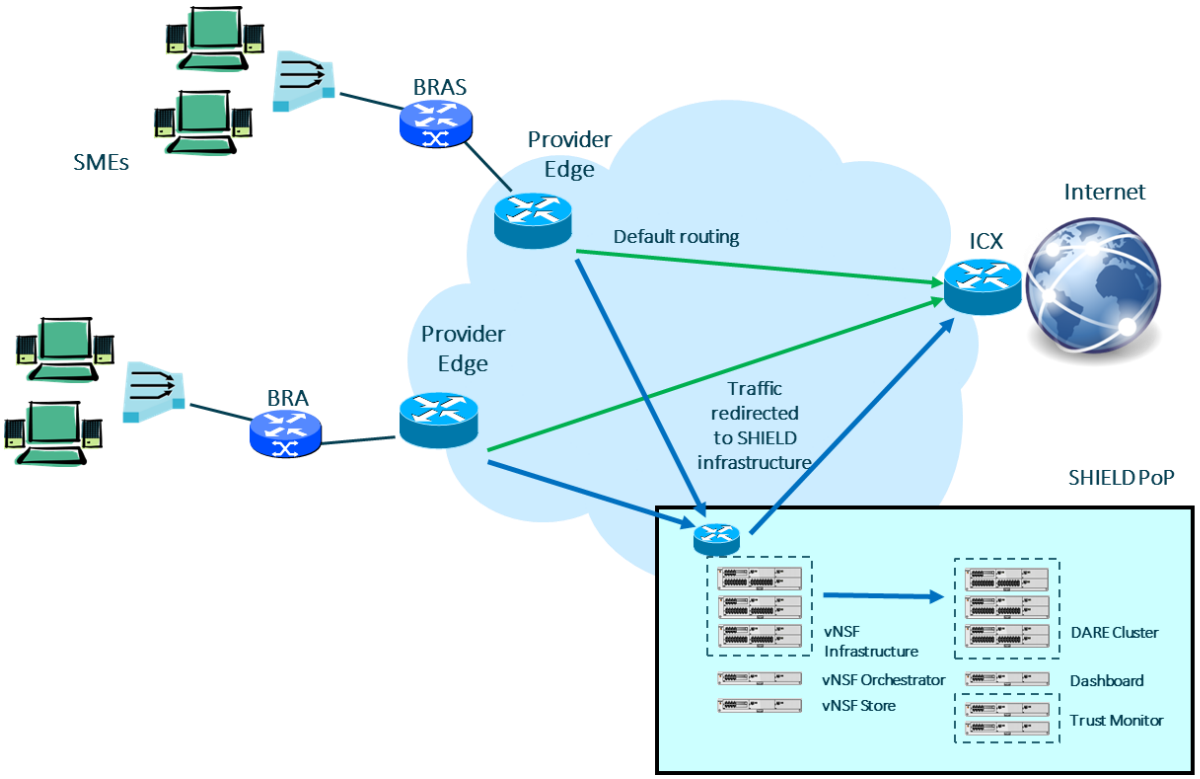


Figure 10. General Infrastructure Deployment Configuration for TSS

The study should distinguish two types of resources according to the network elements used and the topology selected. The physical resources are part of the common infrastructure including any network components used in the TSS model for all the actors and the virtualized resources that are assigned to each VNF and each client.

Initially the resources per service are calculated, they are mapped to infrastructure resource requirements, and finally these are translated into physical resources.

In more detail we have:

Virtualised resources

This type includes virtualised computing resources (number of CPU cores), virtualized RAM, virtualized storage and virtualized networking capability. These are the resources that are allocated to the VNFs and are mapped into physical resources.

Physical resources

This category includes the general purpose ICT resources and specialized hardware used from SHIELD solution. The ICT resources comprise: memory, CPUs, storage and networking physical resources. The physical assets that are part of the SHIELD architecture, include:

- Servers, (incl. memory, CPUs, storage)
- (SDN) switches
- Network connections
- Installations

3.3.1. Dimensioning rules per Case

The main activity includes the installation of resources in a SHIELD Point of Presence (PoP) inside a datacenter of the TSS Operator. Each PoP consists of a number of servers according the dimensioning results. For simple Dimensioning rules one type of physical server per case will be used. The Servers (commodity x86) are capable of running the vNSFs and host the rest components of the SHIELD architecture (vNSFO, Dashboard, DARE, TM).

The Central Office (Point of Presence - PoP) hosts a large number of physical resources. Usually, country-wide operators have a number of them located in geographical dispersed places for security and redundancy reasons. Even for the implementation of NGA networks (FTTC or FTTH) a substantial number of BRAS (Broadband Remote Access Servers) consist in the whole country. In such location, where almost all BB traffic aggregates, a PoP of SHIELD solution could be collocated. We do not envisage the installation of any SHIELD-specific equipment to the client's premises.

In this study, we will assume that there are several PoPs serving the whole area under study (several Local Exchange centers of the telecom operator). Each PoP hosts x86 type servers that serve as a pool for the physical resources. Multiple Point of Presence (PoP) with extra interconnections links are included in the study but inter-PoP traffic is considered as negligible.

All PoPs support the following common features:

- They host the core components of the SHIELD framework (DARE, vNSFO, TM, Dashboard)
- Host the vNSFs
- Include hardware (HW) NFV and TPM capable

The dimensioning of the system was based on observations and measurements from the two pilots which were performed using actual traffic in NCSRD and SPH, with respect to DARE and vNSF resource usage. For the DARE cluster, we assume at least 10C/20T 1TB, 128GB RAM per server for 250 clients and for the vNSF cluster 10C/20T 500GB, 128GB RAM per server for 90 clients. Each server could be equipped with two processors (max 20C per server). The two other major components like TM was based on measurements in HP Labs and Torino labs (TM

monitor need less assistance in terms of Cores, so more clients can be supported). Assuming that traffic is closely related to processing and performance requirements, the number of new servers required annually and their respective cores is calculated by subtracting the capacity of already installed servers from the total traffic requirements and dividing by the capacity of the new servers by taking into account the annual traffic/performance trend for the new servers[15] as well as the DARE servers (calculated separately). However, for RAM, Storage we assume a constant capacity of 128GB, 1TB for the whole study period.

3.3.2. Cost estimations

The cost estimations for the total solution have been made, by taking into account pilot and demo network deployments within the project period including the upgrades that are needed in order to meet a commercial deployment. The approach was to use older collected data and then extrapolate the costs towards a commercial deployment. As already mentioned in the previous sections, the costs are divided into CAPEX and OPEX. In the following sections, the assumptions that have been made for each cost category are presented.

The cost oriented approach is based on Routing factors. The Routing factors describe the usage of network building blocks (the route) by each technical product (or type of the flow). Routing factors are hence the key used to allocate network building blocks cost to technical products (together with Mbps used or number of Clients). Routing Factor information is ideally stored in a network system, but can also be collected through expert opinions from Network staff.

3.3.3. CAPEX estimations

This includes all the costs of purchasing the required components for running the SHIELD services. Concerning the Site (acquisition and preparation), since this costs are related to the preparation of the PoP for a datacentre, this cost has been taken into account as an increment in capex and all related cost of using this infrastructure has been taken into account as OPEX cost (i.e host the servers). Only the installation of the new servers is considered, as well as the required upgrades. For all servers needed, the assumption is that operators have to host them in an existing Data Centre, along with the existing IT and network equipment

The following table shows the CAPEX prices that were used in the modelling at a 2018/9 reference price.

Table 7 CAPEX Cost Components (cost per unit)

Description	Cost
vNSF cluster Server	7,000 €
SDN switch	4,000 €
vNSF Orchestrator	7,000 €
DARE cluster Server	7,000 €
Trust Monitor Server	7,000 €

[15] https://www.karlrupp.net/2018/02/42-years-of-microprocessor-trend-data/

Description	Cost
Billing System upgrade	50,000 €
Data Center (Racks, preparation)	1,500 €
vNSF Store Server	7,000 €

3.3.4. OPEX estimations

The TSS business model assumes that the operator has already a presence in the relative market and is organized with customer support and similar activities like customer acquisition and retention. The OPEX cost used within this study is related to the network operation, IT support for the solution in an incremental basis. Only the OPEX related to the network operation is taken into account, so that it now includes some elements related to the IT support that is expected to increase due to the use of common servers and the cost for developing and maintaining the VNFs and the VMs.

The following generic breakdown has been used in order to distribute the relative OPEX costs:

- Installation procedures
- Maintenance of equipment and components (includes IT equipment that is now a part of the SHIELD solution)
- VNFs development and maintenance (internal or outsourcing according to the Business model followed)
- Network operation and maintenance (incl. operating systems)
- Rental of physical network resources, e.g. the optical network or the network link cost.
- Site rental and electricity costs for the datacenter.

Note: We have not included software licensing costs in the OPEX. Since most SHIELD components are released as open-source, they do not come with a mandatory license fee. However, it is expected that the SHIELD technology providers will be involved in the maintenance and support of the respective components, so their profit will come from the associated OAM contracts, rather from direct licensing revenues. This is further explained below.

The OPEX cost breakdown is important for the definition of the income of all players acting as outsourcing in the present TSS model. The telco in most of the cases contracts the SHIELD installation/integration/maintenance work to a system integrator, rather than implementing it fully with an in-house personnel. In an operator basis environment, as explained above, SMEs can benefit from outsourcing offering (VNFS construction, installation and maintenance, Analytics). Thus all possible actors could evaluate their revenue streams. The NFV technology provider will offer technology solutions for NFV, such as virtualization platforms, NFV management and orchestration solutions, the vNSF developer virtual network security functions and Data Analytics Provider offer data storage and analytics services in order to predict specific vulnerabilities and detect incidents. All OPEX costs related to such activities will eventually generate revenues for the SMEs.

This will be achieved commercially for each role (included in the joint exploitation plans) and the impact for the SMEs involved is measurable and considered to be an achievable target for growth. A quantification of the financial benefits for SMEs, under scenarios will be presented here after.

The cost of the infrastructure includes the cost for the powering and cooling engine of the DC and varies with the type of DC, its size and location. The cost of infrastructure is broken into two factors: one related to the total power of the DC and the other to the required area of the DC. A price of €2,200 per square metre, and an annual cost of €17,000 (for 25 KW) of power are assumed for the area and powering respectively[16]. The cost of electricity consumption is calculated by the total consumption of the DC equipment multiplied by the cost of €0.0788 per kWh, which is the average cost for industrial users across EU countries[17]. We assume the existence of racks with 42U capacity and that each server occupies 1U space on the rack. Using the number or racks, one can easily estimate the required space for IT equipment. This space should be then doubled in order to take into account other equipment requirements and air flows (common practice).

Table 8 OPEX per Cost Component

Description	Cost	Period/Description
vNSF Cluster	5,400.00 €	Yearly per Unit (Salaries + licenses)
vNSF Orchestrator & SDN Switches	4,800.00 €	Yearly per Unit (Salaries)
DARE	4,800.00 €	Yearly per Unit (Salaries)
Trust Monitor	4,800.00 €	Yearly per Unit (Salaries)
Billing/Invoicing	0.30 €	Monthly Per client
Data Center	3,700.00 €	Monthly per Rack (Power and rental)

One major advantage for the TSS model is that the traffic from different clients to reach the entry of data center is basically included in the Broadband subscription. The Datacenter with SHIELD servers will be hosted at several Operator premises (as a big datacenter or PoP near the BRAS). The Operators clients, will use operator core networks to reach datacenter, from diverse PoPs, so no cost it is expected, or will be assumed negligible by the operator (in our model a small amount for the usage of the core network has been included). The example case under investigation is considered to be a service in one country (like SPAIN), and clients from other operators will reach SHIELD datacenter through internet (specifically using national neutral point). This solves wholesale traffic among Operators because each operator paid by a global

[16] In a real environment with 10 rack half full we have 25 kWh, per hour (17,000 € per year)
[17] Electricity prices for non-household consumers

bandwidth to be connected to the neutral point for all their services, independent of the type of traffic.

Finally the SHIELD platform should be prepared as a product the first year of the study. Extra cost has been included for the productization of the SHIELD components.

3.4. Results and Analysis

The results presented will focus mainly on Net Present Value (NPV) and Cash Balance. If the NPV is positive, the project is acceptable and it is a good indication for the profitability of an investment project, taking into account the time value or opportunity cost of money, which is expressed by the discount rate.

Figure 11 illustrates the share of accumulated CAPEX and OPEX in the costs of investment during the study period for a large country. The results are less than ¼ in Capex and more than ¾ in OPEX which is quite logical for a project based on NFV/SDN technology. Figure 12, Figure 13, Table 9 and Table 10 summarizes the cost breakdown per component during the study period.

The biggest investment corresponds to the cost for acquiring the servers for the vNSF cluster (Server, cores, ram, storage) and the cost for the DARE cluster having a total share of more than 73% of total accumulated CAPEX. Particular cost is the acquisition of the TM and the preparation of the extra space in the Datacenter in connection with the SDN switches.

Additionally, the cost for supporting the vNSF services, DARE (Security Analytics) and TM are more than 70% of total accumulated OPEX. This cost represents the maximum value that the TSS operator could subcontract in other players like small SMEs specialized in NFV technology, vNSF developers and Data Analytics specialists. Most of these costs represent personnel cost in added value for the collaborating SMEs in the TSS model. These revenues are illustrated in Figure 13 in ascending order. The major cost is the possible maintenance and licensing of the vNSF cluster.

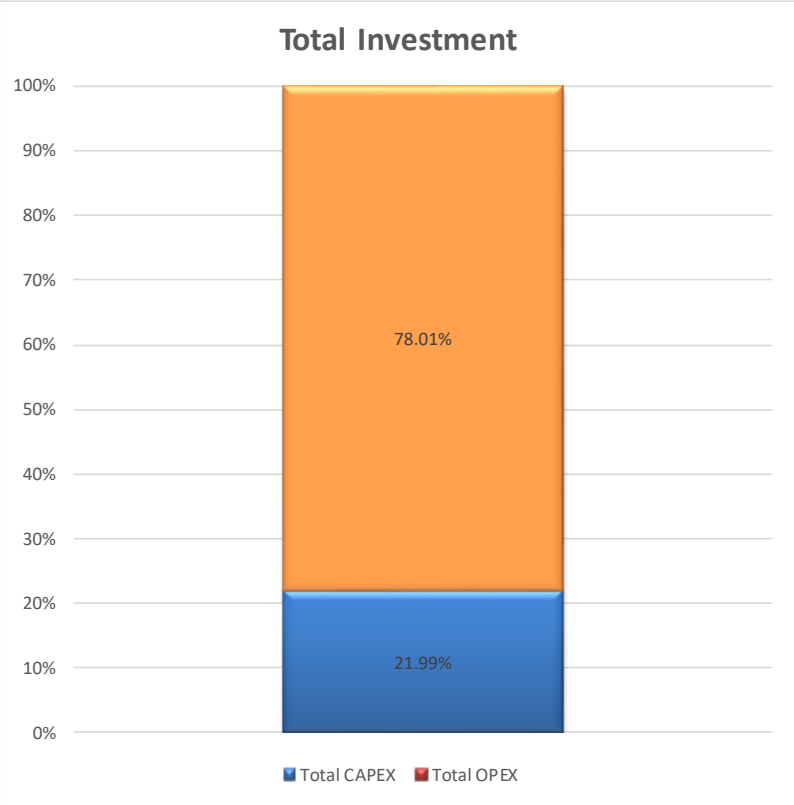


Figure 11. Percentage of CAPEX and OPEX in total investments.

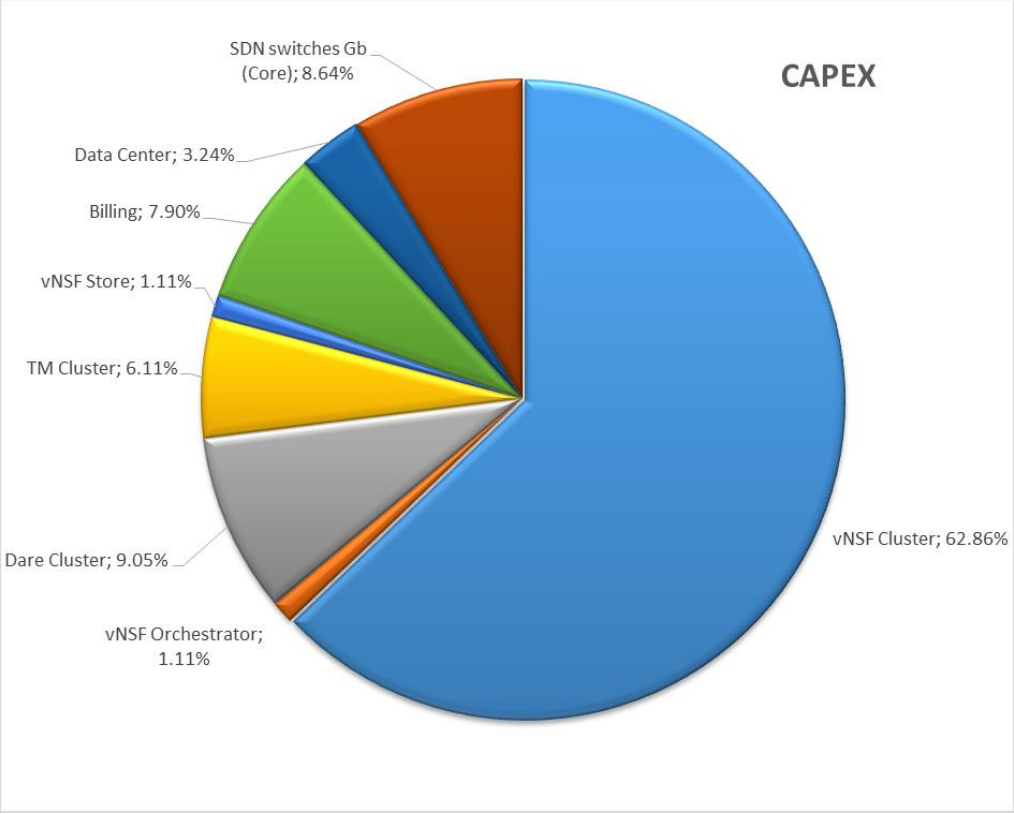


Figure 12. CAPEX Breakdown in total investments.

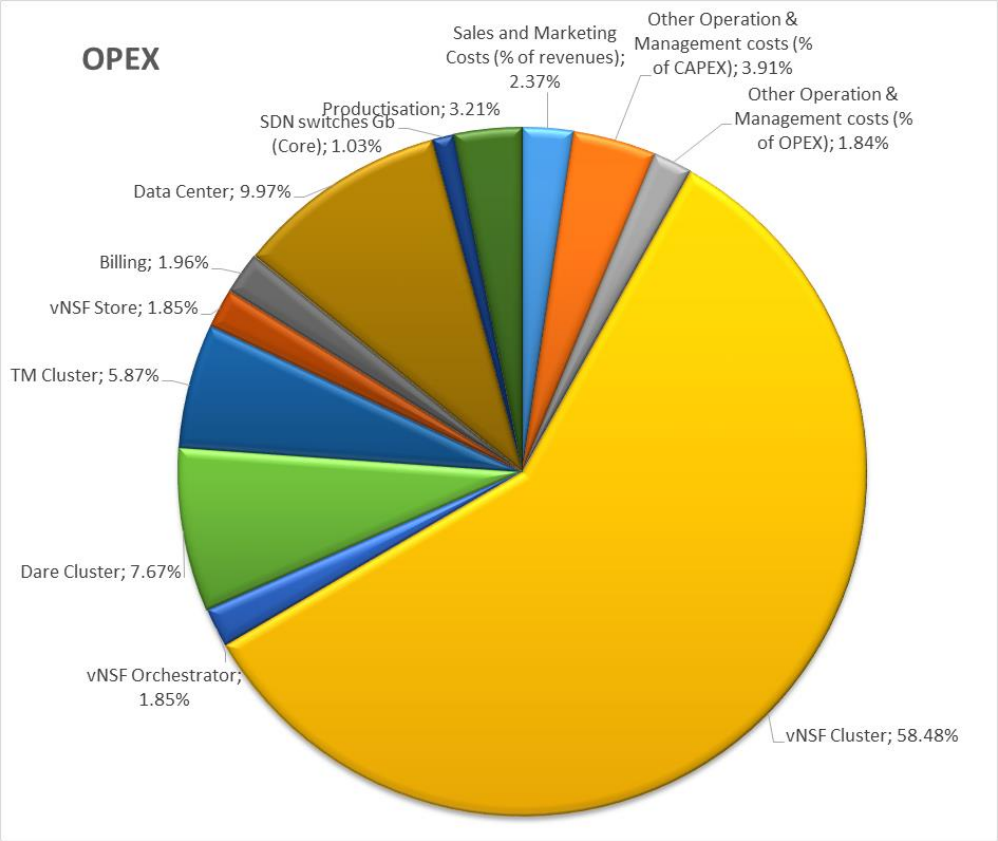


Figure 13. OPEX Break down in total investments.

Table 9 Main Cost Component Total Capex

Elements	% of total CAPEX	Value
vNSF Cluster	62.86%	397,753 €
vNSF Orchestrator	1.11%	7,000 €
Dare Cluster	9.05%	57,263 €
TM Cluster	6.11%	38,650 €
vNSF Store	1.11%	7,000 €
Billing	7.90%	50,000 €
Data Center	3.24%	20,474 €
SDN switches Gb (Core)	8.64%	54,650 €

Table 10 Main Cost Component Total OPEX

Elements	% of total OPEX	Value
Sales and Marketing Costs (% of revenues)	2.37%	53,250 €
Other Operation & Management costs (% of CAPEX)	3.91%	87,827 €
Other Operation & Management costs (% of OPEX)	1.84%	41,253 €
vNSF Cluster	58.48%	1,312,925 €
vNSF Orchestrator	1.85%	41,512 €
Dare Cluster	7.67%	172,126 €

TM Cluster	5.87%	131,677 €
vNSF Store	1.85%	41,512 €
Billing	1.96%	44,088 €
Data Center	9.97%	223,803 €
SDN switches Gb (Core)	1.03%	23,028 €
Productisation	3.21%	72,000 €

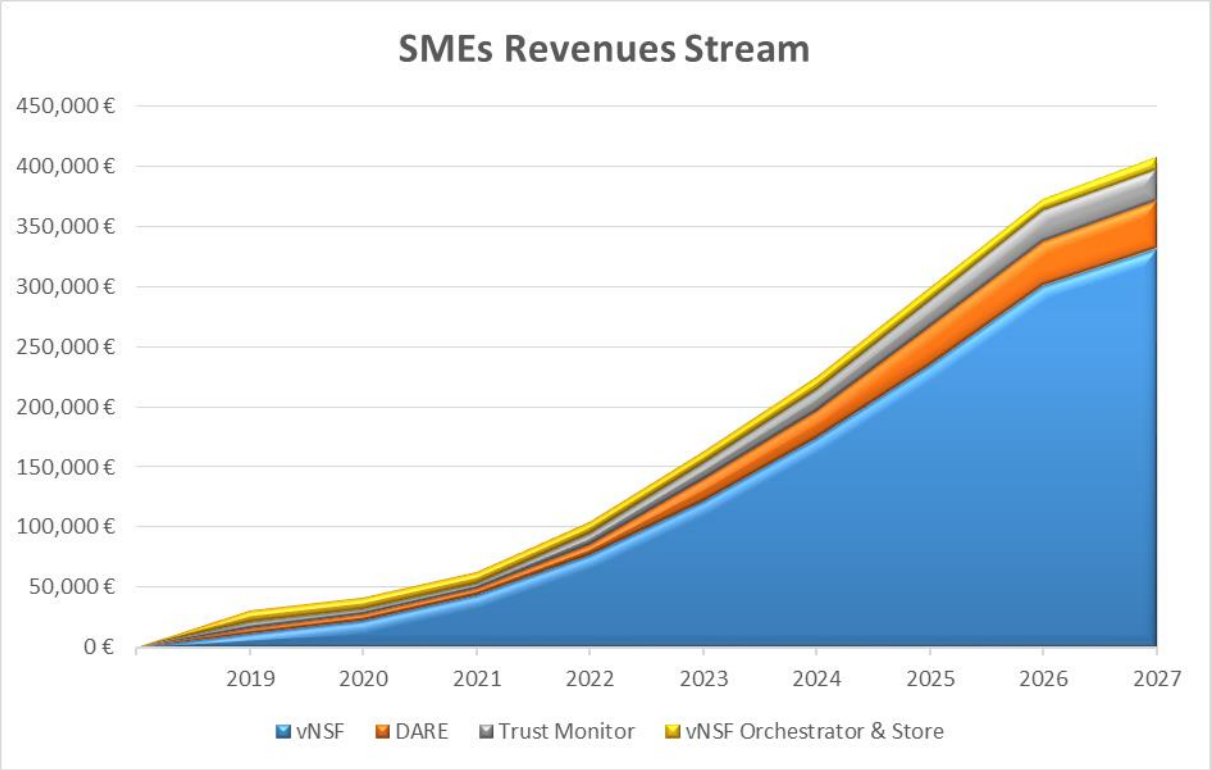


Figure 14. Revenues Streams break down for collaborating SMEs in the Business Model.

Our scenario features an operator with a market share of 33% in a large country area. In the case where the ARPU for SHIELD solution (full package) is at 30€, it is noticeable that the cash balance turns positive after 7.5 years (6 years operation and one preparation of the SHIELD product finalization and Operator set up). The pay back periods are generally around 7 years, which is not considered too long against the magnitude of the project. The project represents an NPV equal to 75,000 €, or 220,000 € including the rest value and an IRR of ~17.44%. With respect to the select ARPU Values the profitability is risky but if we select 40€ for the Full SHIELD solution the results are quite promising. Having a NPV close to 520,000 € (671,000€ with rest value), leads to an IRR more than to 41% and a payback period almost five (5) years (the results are presented in Figure 15). The most promising economic indicator is the shape of the cash balance. Since the lowest part is not so deep the total amount of investment remains low as well as the total risk for the player (TSS and the collaborative SMEs). It is important to emphasize that the offering of 4 different packages with 4 tariffs spread in the total number of clients gives less profitability than the offering of a single package for all clients since 50% of the clients will pay a lower ARPU.

For our scenarios, we have calculated the minimum monthly ARPU required for NPV to be equal to zero at the end of the study period (28.36€ - ARPU required for zero NPV). These results can be used as an indicator of the cost of service for each subscriber according the Tariff Structure of the basic tariff (Gradient) (Table 6). The study shows that the NFV/SDN business cases can be positive for TSS operators with substantial market share (~30%) in typical large European countries. TSS model could be profitable in most cases for established operators with reasonable market share since the structure of the investment in IT and network components graduate according to the number of the clients and the traffic generated.

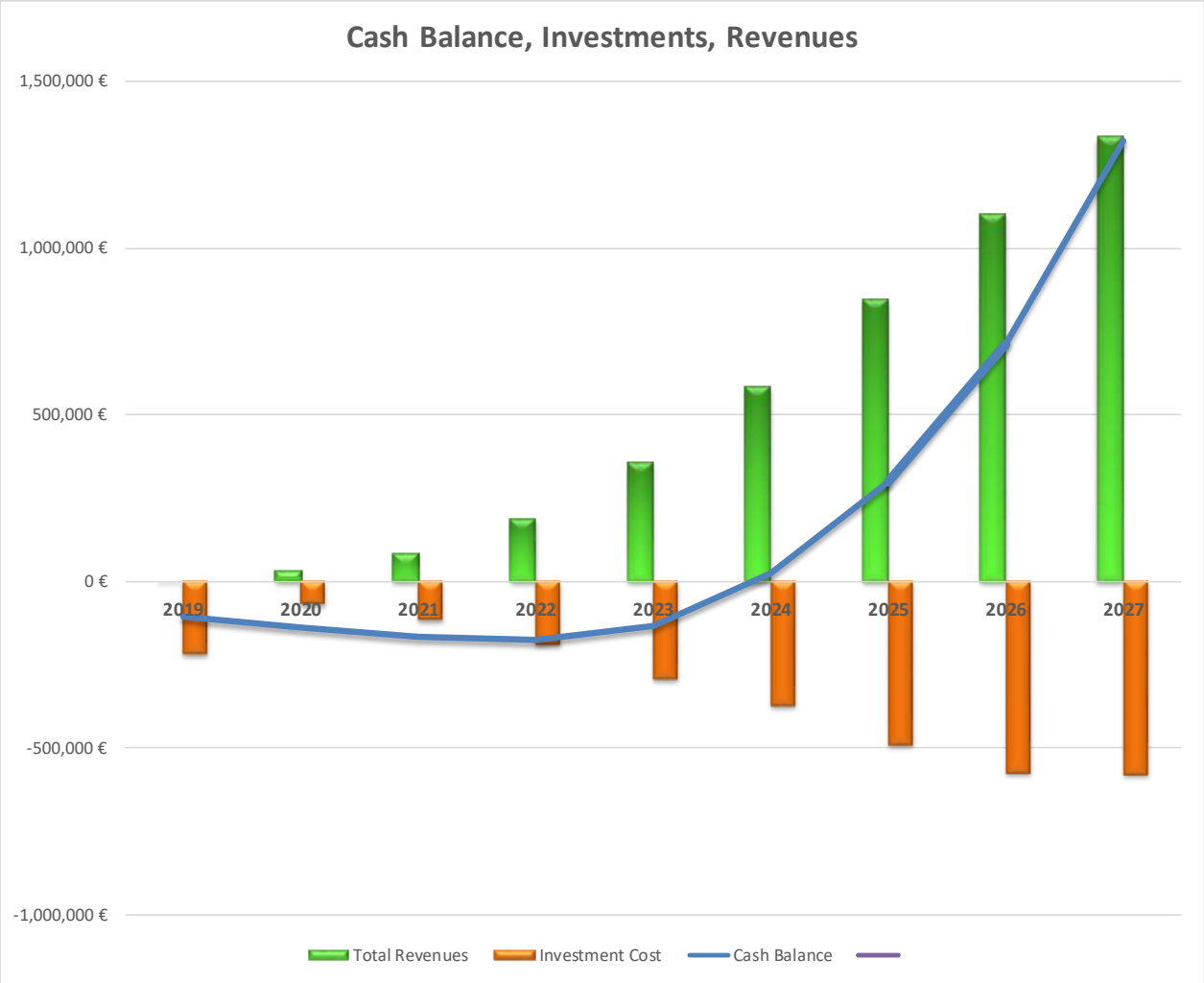


Figure 15. Revenues, Investments (CAPEX, OPEX) and Cash Balance for ARPU equal to 40 euro (full SHIELD package).

3.4.1. Sensitivity Analysis

For better understanding of the impact of the market share on the feasibility of the SHIELD solution we examined the case of a market with more players and for various market shares of one of the modelled operator (like the TSS). Figure 16 illustrates the cash balance (cumulative cash flows of the PVs) for different Market Share assuming ARPU equal to 40 euros. In all cases, the gradient of the cash balance curves at the end of the study period indicate the future earning potential. Another key point is the maximum finance needed (lowest point of the curve) quite similar to all cases provided that the upgrade into the system for offering an expansion of services is affordable.

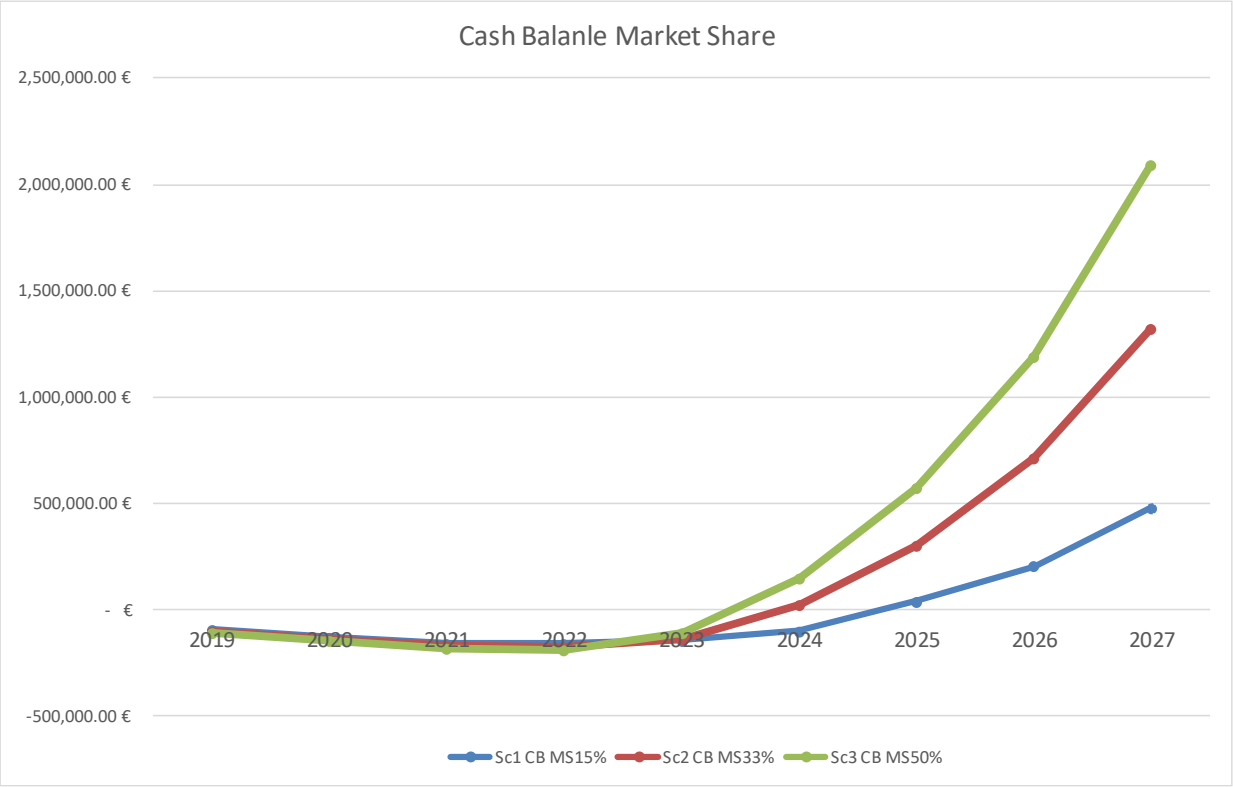


Figure 16. Cash Balance under different Market Shares.

Demand and penetration are the main factors which cause risks related to telecom and IT investments. The higher the penetration of the potential customer base is, the higher the profitability of the investment becomes. Moreover, if the penetration does not reach the critical mass that is required for the creation of the new cybersecurity based services market, the investment may not even be profitable at all.

Operators with a market share of around 9% (base value 33%) experience a negative NPV during the window of the time study; however, if we extend the study time window by one more year then the calculated NPV becomes positive. The results reveal that since the expenses (for deploying and running) are high there must be a sufficient amount of revenues for the

project to be financially viable. On the other hand, for operators with a large market share (50%), it seems that the expected revenues will ultimately overcome the expenditure within a reasonable time frame (less than 5 years). Furthermore for a take-up rate of almost 3% (compare to the 10% Figure 7. Forecast of Security Services (S- Curve)) the business case became non profitable. This percentage is considered as too low for the evolution of managed security services. Another critical parameter for negative NPV it the traffic evolution of SMEs subscribers. An increased traffic profile more than 20% per year (12% per year in a conservative forecast) gives negative NPV.

In order to better estimate the factors affecting our business case we have also performed a sensitivity analysis on the following parameters:

- ARPU (Tariff) / month (euro)
- Clients per vNSF (per two cores per server)
- Mean traffic per Client (Mbps)
- Servers Opex (Total OPEX cost %)
- Expected Take-up 2035 (10%)
- Target Market Share (33%)
- Business SMEs (total addressed SMEs in the country)
- Traffic Increase (12%)
- WACC (%)
- Servers Cost (Total Capex Cost %)
- Annual Tariff Degression
- Taxes
- Clients per DARE servers

Each of the parameters was changed to the value indicated in the graph (-20%) and (+20%) from the values used in the base case. So for the most important parameters (that will be selected for the Risk Analysis as well) the conclusion are quite interesting. The most influencing variable is the ARPU as was expected (generated from monthly tariff). The monthly tariff is the most critical parameter but even for a -20% reduction the project remains profitable. It reflects the degree of competition within the value chain. The SMEs clients served per server is a critical parameter for dimensioning and profitability indication. Our dimensioning rules are robust since the project does not end to a negative value even with 20% increase in the clients' total number into the vNSF cluster. The total OPEX cost as expected is more critical for the total NPV from the total Capex since the contribution of OPEX cost in the total investment cost is more than 78%. As a conclusion ARPU, served clients per vNSF, and traffic generated from the SMEs have the strongest effects on the NPV, followed by the Demand and OPEX, while traffic increased per year, WACC and Taxes have a minor effect. A reduction in total penetration results not only in lower revenues but also lower costs due to less investment needed

Table 11 Sensitivity Analysis (-20%, +20% from the base value)

Input Variable	-20% NPV	+20% NPV	Base Value
ARPU (Tariff) / month	165,616 €	884,733 €	40 €
Clients_vNSF	308,997 €	677,324 €	180 €
Mean_traffic	705,480 €	347,760 €	5 €
Servers Opex	671,841 €	379,127 €	100%
Expected Take-up 2035	394,599 €	658,213 €	10%
Target Market Share	394,599 €	658,213 €	33%
Business SMEs	394,599 €	658,213 €	100%
Traffic_incr	645,544 €	389,662 €	12%
WACC	632,853 €	435,797 €	12%
Servers Cost	596,458 €	455,152 €	100%
Annual Tariff Degression	581,645 €	471,529 €	3%
Taxes	567,826 €	483,784 €	20%
Clients_DARE	497,542 €	542,631 €	500

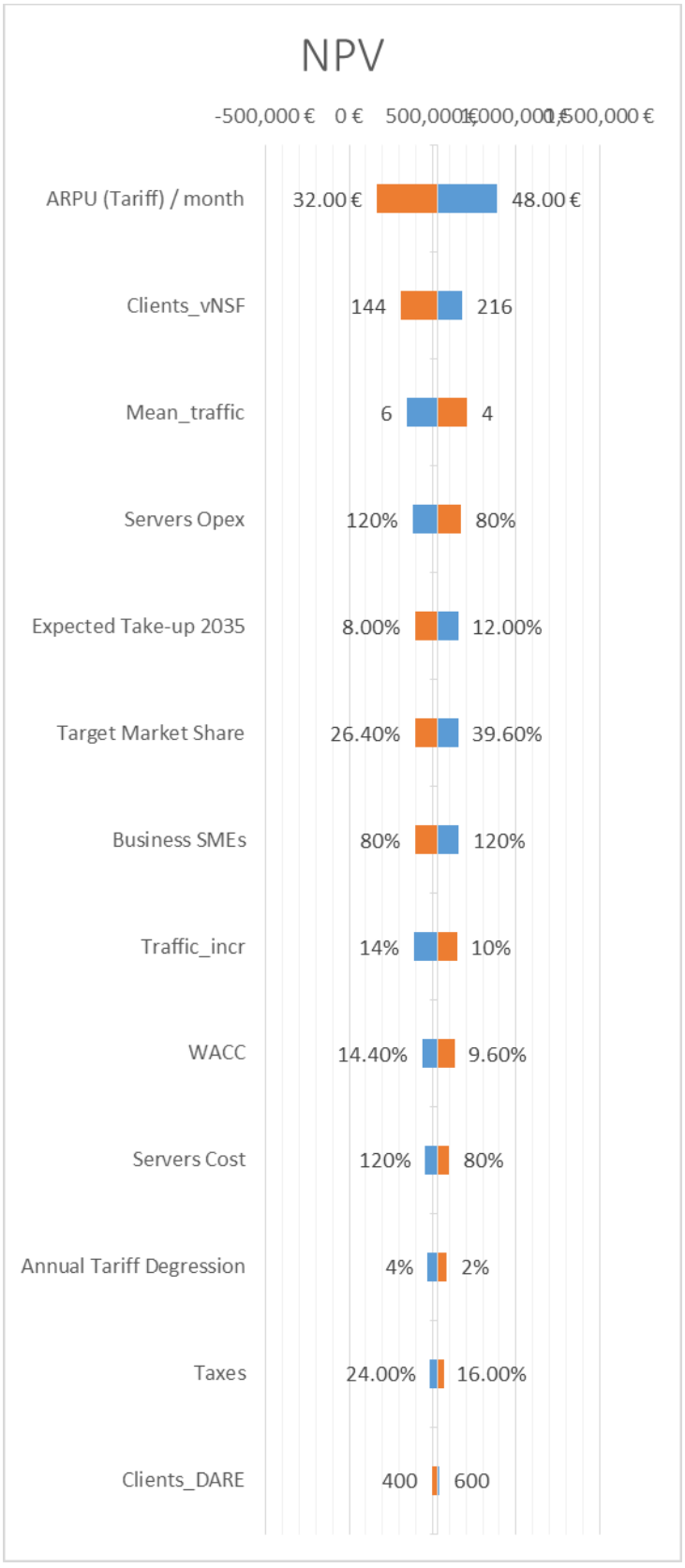


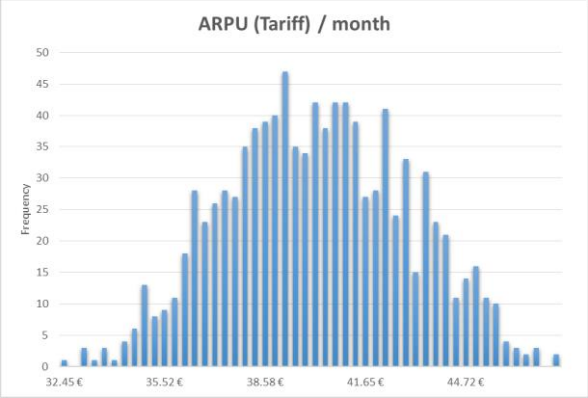
Figure 17. Sensitivity Analysis Results

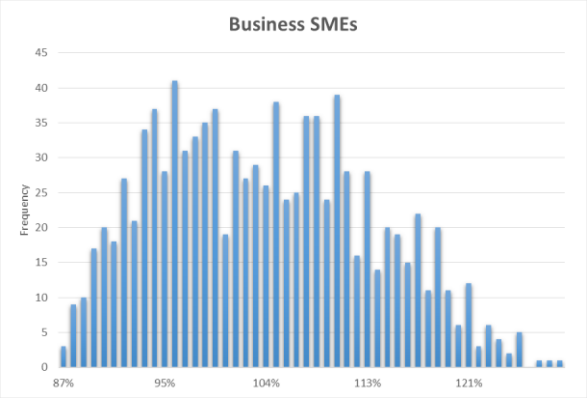
3.4.2. Risk Analysis

For the parameters that were used in the sensitivity analysis a risk analysis was performed for the NPV. For each of the input parameters a probability distribution function (PDF) was selected in order to model the uncertainty using the Beta distribution. A pessimistic scenario was selected in which all the parameters could change in the way that lower the NPV, the profiles that were used to model the PDFs are presented in **Error! Reference source not found.**. Based on these profiles the parameters (alpha and beta) of the Beta distribution were selected. The following figures illustrate the PDF selection for each of the parameters. Then a Monte Carlo analysis was run for 1,000 to 10,000 samples.

Table 12 Risk Analysis Profiles

Parameter Beta Distributions for Risk & Sensitivity Analysis						
Parameter	Estimate, default	Min	Lower conf.	Upper conf.	Max	Confidence
Expected Take-up 2035	10.00%	5.00%	7.00%	15.00%	20.00%	90.00%
Target Market Share	33.00%	15.00%	20.00%	45.00%	60.00%	90.00%
Traffic_incr	12.00%	8.00%	10.00%	15.00%	20.00%	90.00%
Mean Traffic	5	2	4	7	8	90.00%
Business SMEs	100.00%	85.00%	90.00%	120.00%	130.00%	90.00%
ARPU (Tariff) / month	40.00 €	30.00 €	36.00 €	45.00 €	50.00 €	90.00%
WACC	12.00%	9.50%	10.50%	13.00%	13.50%	0.00%
Server CAPEX	100.00%	80.00%	90.00%	110.00%	115.00%	90.00%
Server OPEX	100.00%	80.00%	90.00%	110.00%	115.00%	90.00%





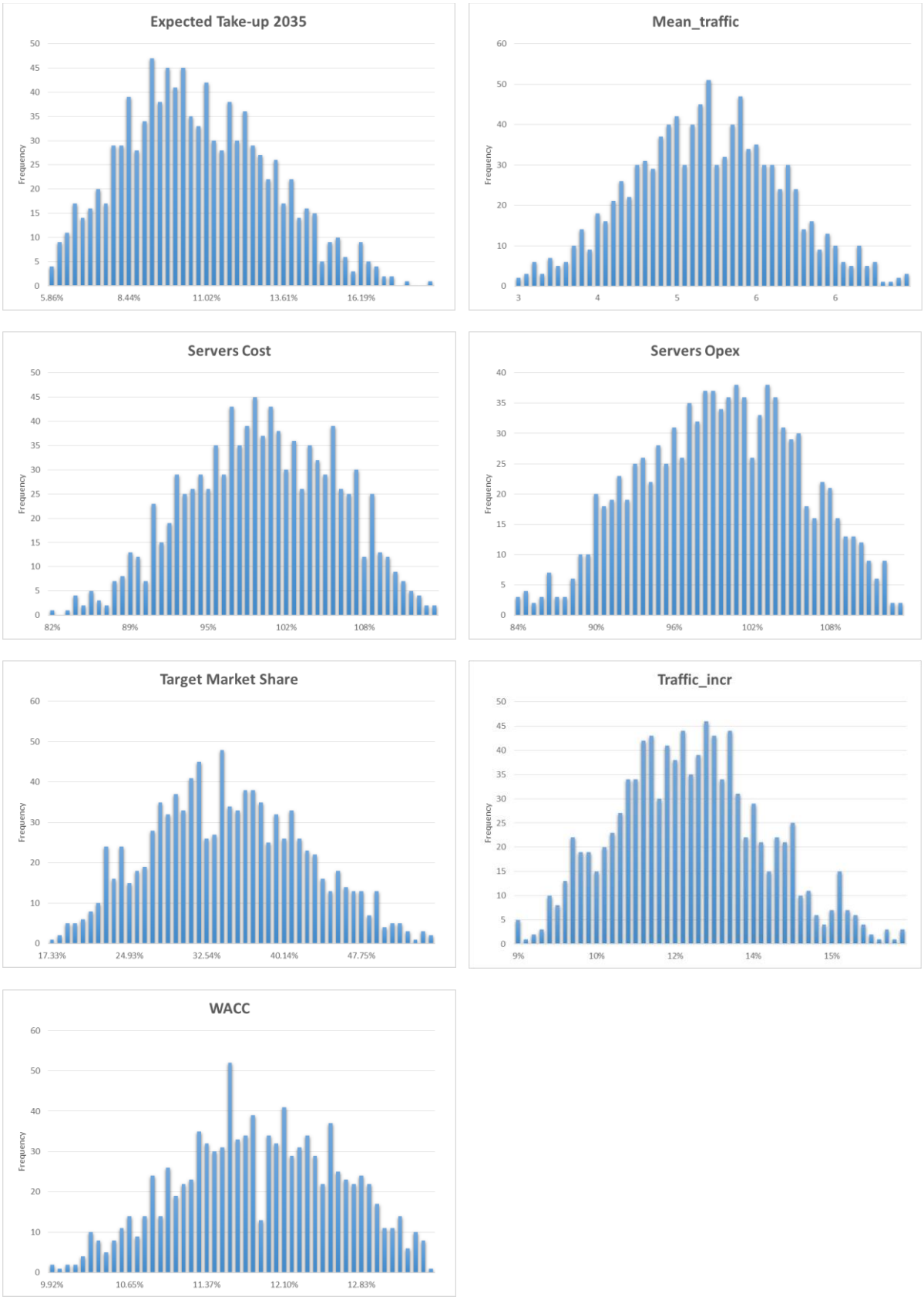


Figure 18. PDF distribution of Parameters.

The extensive risk assessment has been performed on the different tariff scenarios, demand technical and cost parameters. The result is with certainty greater than 90% a positive NPV at

the end of the study period. Risk analysis results are presented in Figure 19. The results of the risk analysis are presented in Figure 19. The mean value of the NPV is equal to 610,351.61 € and there is a 90.5% percentage that the value of NPV will be positive. These results seem promising, taking into account that the input parameters were generally on the pessimistic side. This information will give the opportunity to the decision leaders to invest in the selected technology since the risk is quite low compare to other telecom or IT projects.

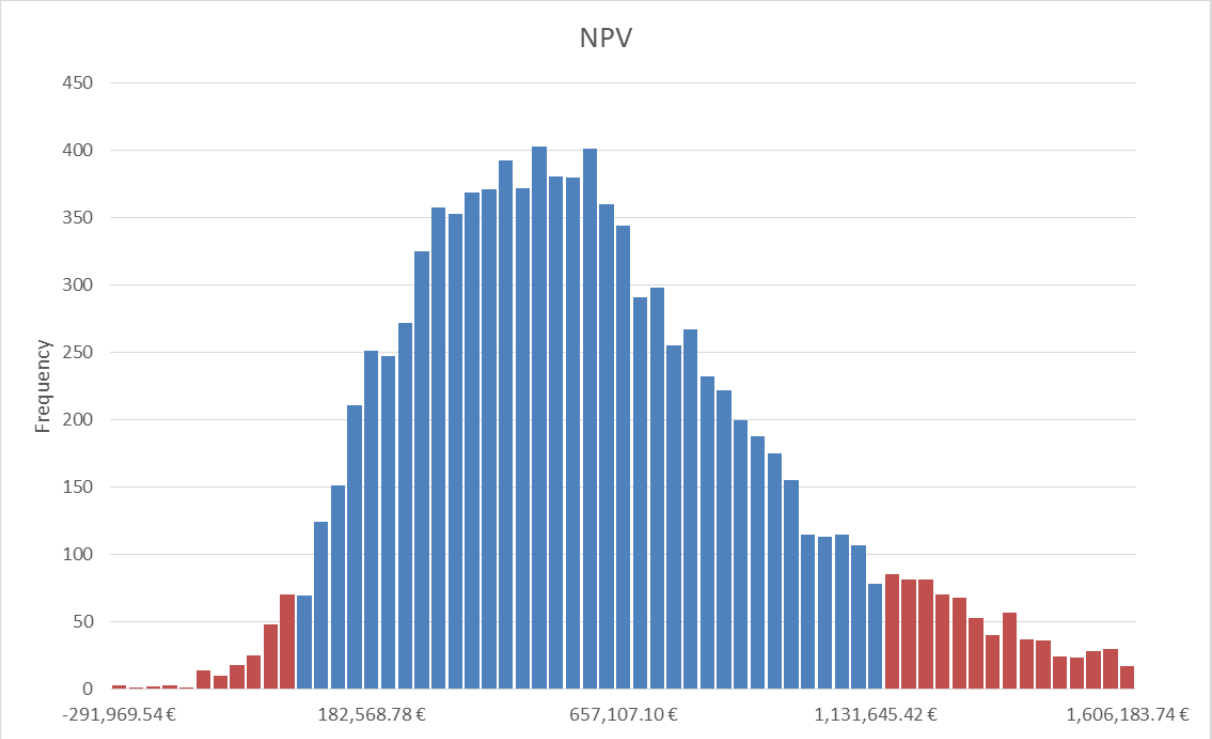


Figure 19. PDF distribution of NPV (90% certainly)

The median value of the NPV is equal to 558,359.85 € and with a 90.5% percentage that the value of NPV will be positive the range is from 26.360 € to 1.156.741 €. The negative values are calculated only for input parameters in the downside (all at the same time). Likewise the percentiles analysis shows that 50% of the NPVs values are greater that the base value results presented in the base case scenario (520,000 €) and 80% of the cases greater than 317,000 €.

4. EXPLOITATION PLANS

This chapter presents the Final exploitation plans of each partner as well as the joint exploitation plan for the primary selected business model (TSS) and selected products and services.

4.1. SHIELD final results and owners

Prior to the elaboration of the exploitation plans, it is necessary to review the main results of the project as well as the assigned IPRs. Table 13 below includes an (updated) identification and association of results. In the case of the joint results, the amount of the share of each partner will be decided prior to any commercial exploitation.

Table 13. SHIELD results and IPR holders

Exploitable result	IPR holders	Release	License
Res.1 (SHIELD architecture and specs)	All SHIELD partners (joint result)	Public	Copyright
Res.2 (vNSF Store)	UBI, TID, I2CAT (joint result)	Public	Open-source / Apache
Res.3 (vNSF Orchestrator Platform)	I2CAT, TID, UBI, ORION	Public	Open-source / Apache (incl. background from other open-source projects)
Res.4 (Information-driven engine)	INFILI, SPH, I2CAT, POLITO (joint result), TALAIA	Public /Proprietary	Open-source / Apache (incl. background from other open-source projects), Proprietary (TALAIA foreground)
Res.5 (SHIELD Dashboard and billing framework)	UBI	Public	Open-source / Apache

Exploitable result	IPR holders	Release	License
Res.6 (Attestation framework)	POLITO, HPELB, TID	Public /Proprietary	Open-source / Apache, Proprietary (HPE foreground)
Res.7 (vNSFs and security services)	ORION, TID, i2CAT, POLITO, NCSRD (individual vNSFs)	Public	Open-source / Apache

4.2. Join Exploitation Plans

4.2.1. Joint exploitation plan for the SHIELD offering as the TSS enabler platform

The primary joint exploitation plan of the project has been elaborated on the basis of the Telecom Security Service (TSS) business model, which has been identified as the most prominent one for SHIELD.

The plan foresees that the SHIELD framework is offered as a TSS enabler platform to telcos and large enterprises who wish to provide TSS services to their customers. Three deployment options are foreseen:

- Option 1 - NFV SecaaS (basic) configuration: this configuration will enable the telco to host and deploy on-demand virtual security services
- Option 2 - NFV SecaaS + DARE configuration: this configuration will enable the telco to host and deploy on-demand virtual security services plus rich security analytics for incident detection/classification and automatic remediation
- Option 3 - NFV SecaaS + DARE + Attestation configuration: this configuration will enable the telco to host and deploy on-demand virtual security services plus rich security analytics for incident detection/classification and automatic remediation, as well as infrastructure and service attestation.

It is expected that the candidate customer (telco or big enterprise) will prefer to contract an ICT partner for the installation, configuration and maintenance of the SHIELD platform in their premises, rather than undertaking it with in-house resources.

In this view, a partner from the SHIELD consortium will undertake the role of the system integrator/prime contractor and establish the contract with the customer (telco). SPH is a likely candidate for the role of the prime contractor, given its strong background as ICT system integrator and the references it has from similar projects in the telco industry. HPE and TID can also undertake such a role, given their reputation and global footprint.

The prime contractor will take the following steps to secure a successful deployment of the SHIELD technology:

1. Liaise with the customer in order to understand their needs and constraints

2. Propose a proper system configuration to be deployed and identify the developments which might be needed
3. Contact the associated technology providers/IP holders:
    a. I2CAT, UBI, ORION, TID, NCSRD, POLITO for Option 1 (depending on the security services to be available)
    b. Above partners plus INFILI for Option 2
    c. Above partners plus INFILI and HPE for Option 3
4. Negotiate with each partners the price and terms for:
    a. the software licensing,
    b. the developments which might be needed
    c. the subsequent operation and maintenance tasks
5. Present an integrated offer to the customer – and possibly further negotiate
6. Upon offer acceptance, manage the preparation and establishment of the main contract and subcontracts (to the SHIELD partners)
7. Upon contract establishment, act as Project Manager / single-point-of-contact for the customer, supervising all tasks related to the deployment (and subsequent maintenance) of the SHIELD solution in the customer's premises.

4.2.2. HPELB-POLITO-TID joint exploitation plan: Trust Monitor as-a-Service

In deliverable D2.3, we identified and presented the business model for the Trust Monitor as-a-Service (TMaaS). HPELB, POLITO and TID plans includes bringing the Trust Monitor to market as a service.

To this end TID identified 2 specific markets in the telco ecosystem that could leverage the attestation feature of the Trust Monitor:

- Security-sensitive clients (e.g. military, other government agencies and banks) that wants to verify the correctness of the vNSFs being used;
- Clients that want to migrate from hardware appliances to virtual appliances (vNSFs), whist maintaining the requirement to have hardware-based proof of the vNSFs used. The envisioned markets are lawful interception and content delivery network providers (for their caching appliance).

POLITO is interested in transferring their prototype, which is open-source, and knowledge to a company, such as Hewlett Packard Enterprise/Aruba, that will be in charge of the industrialization and commercialization of the technology as a product.

4.2.3. HPELB-POLITO joint exploitation plan: vTPM development

Following the visit of a POLITO's researcher in HPELB – for 3 months at the end of 2018, HPELB and POLITO started a collaboration on the development of a new virtual TPM (vTPM) approach, taking into account the new TPM2.0 functionality and to address the new industry requirements such as the ability to leverage the physical TPM for multiple vTPMs. HPELB and

POLITO are setting up a collaboration agreement that will extend beyond the SHIELD end date in order to continue the research and demonstrator development. In addition to publishing the research and to create joint Intellectual Property (e.g. patents), HPELB and POLITO are planning to present this new approach to the Trusted Computing Group Virtualized Platform working group. The goal is to include our propos in a future vTPM specification.

4.3. Individual Exploitation Plans

4.3.1. HPELB

Hewlett Packard Labs (HPELB) is the research organisation of Hewlett Packard Enterprise (HPE): its charter is to research new technologies, prototype them and then transfer them to the different business units responsible for developing the customer products. HPELB exploitation plan mainly focuses on transferring the pilot and concept inside HPE's business unit, which are the entity responsible for developing the products that go to market.

Particularly, HPELB wanted to demonstrate the feasibility and effectiveness of Trusted Computing in the next generation of infrastructure that are based on virtualization technologies and are software-driven. This means that HPELB focused mainly on two aspects of SHIELD for its exploitation:

1. Understanding and developing the required enablers – at the platforms level, so that the Trust Monitor can gather securely and efficiently the data it needs to assess the trustworthiness of a platform of the infrastructure. One exploitation is the upstreaming of a Linux patch to enhance the TPM performances for all Linux-based platforms [14]. Following the development work done in SHIELD by HPELB, Aruba (HPE's networking business unit) led the writing of the specification (currently under public review – since May 2018 - and pending publication) of a SNMP MIB for retrieving TPM measurements [15]. HPELB is also contributing to the development of additional TCG specifications, but those are currently confidential to TCG members.
2. Demonstration of the Trust Monitor in order to drive the industry towards secure monitoring of infrastructures using Trusted Computing technologies.

4.3.2. I2CAT

I2CAT has reached an agreement with the Catalan Agency for Cybersecurity (CESICAT) in order to develop the proof-of-concept done in SHIELD with the Autoencoder Neural Network for anomaly detection. I2CAT and Cesicat will together improve the algorithm training it with the data from the network of the Catalan Government (Gencat.cat) to implement it as part of the Intrusion Detection System of Cesicat.

Next exploitation plans include the patent of the improved algorithm and the implementation of a success case with a Cybersecurity Agency. In the future, we I2CAT expects to be able to either transfer the algorithm to a Cybersecurity SME or create a Start-up by its own.

Moreover, I2CAT expects to continue selling its knowledge in OSM by offering consultancy services to companies (especially SMEs) willing to adopt OSM for their own networks.

4.3.3. inCITES

inCITES as a consulting and market research company supports organizations and enterprises in decisions making about the edge technologies of the telecommunications industry. inCITES takes advantage of the project's results to enhance its future market reports and seminars related to Cyber Security in modern networks, with specific focus on business cases modelling analysis and identification of factors affecting the evolution of the specific market. Within SHIELD inCITES improves its methodology and skills for the identification of critical parameters affecting new products entering into a market aiming to support new players to design their solutions in a more efficiently way. In addition inCITES improves during the two year period their portofilo of consulting services as well as its online services and intensify its position as a reference international center of excellence for cybercrime from the business perspective.

4.3.4. INFILI

Infili is a research-intensive SME headquartered in Athens, Greece, that utilizes a unique combination of high-end technologies as an outcome of many years of R&D experience. The company is designing solutions for vertical industries with diverse and very demanding requirements regarding the exploitation of their information and knowledge repositories. Infili researches and develops methods and tools which support information and data services such as Information Extraction and Aggregation, Information Filtering, Recommender Systems and Web Mining. Moreover, it applies technologies for the fast and accurate analysis of large data sets derived from different sources by exploiting a variety of frameworks to build an operational environment that allows for the creation of scalable machine learning applications. Infili's exploitation plan is suggested to be based on the following pillars which are introduced down below:

- For the short term, the DARE platform, which utilizes a plethora of open-source technologies and frameworks to offer a SecaaS solution, is planned to be used as the foundational infrastructure for R&D purposes, such as the development of network anomaly detection and classification methods that will increase the engine's value and broaden SHIELD's impact. During the course of the project, Infili had the opportunity to work towards the development, implementation and evaluation of several scalable analytics models, gaining valuable insight with regard to their efficiency and maturity in production-level deployments.
- For the long term, Infili intends to promote and offer the DARE platform as a comprehensive network monitoring tool to other organisations, taking advantage of its SaaS features that allow for instant deployment, without the need of hardware installation and configuration. It is expected that in the near future, a hybrid approach combined by analyst-driven solutions and state-of-the-art, machine-learning detection systems will become the main way of combating network threats in enterprise environments [16]. This comes in compliance with the modern cybersecurity paradigm which seems to be shifting from threat prevention, adopting a threat detection and remediation model instead. This model emphasizes finding penetrative threats, mitigating the damage they cause, and removing them from the network by prioritizing threat intelligence, threat monitoring, security event correlation, and alerting.

4.3.5. NCSRD

NCSRD, in terms of exploitation, sees a clear link between the participation in SHIELD and the numerous activities of the lab in the domain of 5G (the NCSRD research group was involved in a number of 5GPPP Phase 1 and Phase 2 projects and currently is coordinating 5GENESIS, one of the three "flagship" EU projects on 5G experimentation facilities). Via these projects and also through the coordination of the successfully completed FP7 T-NOVA flagship project on NFV/SDN, NCSRD has already acquired a strong reputation in the area of software networks, which it aims to expand towards the security domain. This will enable the NCSRD research group to enhance its technology offerings portfolio with cybersecurity-oriented software network architectures (e.g. enhancing the NFV MANO stack with security features) and novel, security-oriented Virtual Network Functions (VNFs), which are considered an essential element of future networks. This is expected to improve the NCSRD competitive position for pursuing new funding opportunities in H2020 and beyond. In the academic domain, these results will be exploited towards new PhD theses and dissertations, as well as scientific publications to journals and conferences.

4.3.6. ORION

Orion's exploitation plan focuses on the further development of company products and achieving sustainable growth. It is designed on the basis of the individual exploitable assets developed by Orion, namely the virtual security functions developed for SHIELD and the existing testbed infrastructure.

Gartner[18] predicts the worldwide public cloud services market will grow 18% in 2017 to $246.8B, up from $209.2B in 2016. Infrastructure-as-a-Service (IaaS) is projected to grow 36.8% in 2017 and reach $34.6B. Software-as-a-Service (SaaS) is expected to increase 20.1%, reaching $46.3B in 2017. Gartner also predicts that the Cybersecurity Awareness market has experienced greater than 55% growth from 2014 through 2015 and is currently projected to continue at a similar rate as 2016 draws to a close, with projected 2016 market size of approximately $240 Million. With a promise to drive significant CapEx and OpEx reductions, NFV is poised to transform the entire telco infrastructure ecosystem. Mind Commerce[19] estimates that global spending on NFV solutions will grow at a CAGR of 46% between 2014 and 2019. NFV revenues will reach $1.3 Billion by the end of 2019.

Gartner[20] has defined the integrated threat intelligence and response capabilities in a single flow, as SOAR (Security Orchestration, Automation and Response, see subsection 2.2). ORION's goal is to ensure that NFV products can easily be integrated in such workflows, by adhering to known protocols and developing additional threat intelligence capabilities as part of a SOAR platform.

Orion positions itself in these growing markets, including (but not limited to) the following value propositions:

[18] https://www.gartner.com/newsroom/id/3616417

[19] https://www.prnewswire.com/news-releases/the-network-functions-virtualization-nfv-market-business-case-market-analysis--forecasts-2014---2019-232479091.html

[20] https://blogs.gartner.com/anton-chuvakin/2018/02/22/our-security-orchestration-and-automation-soar-paper-publishes/

Use of existing infrastructure for cybersecurity training & penetration testing: as the need for cyber security awareness and training continues to rise, Orion aims to exploit the developed testbed to plan future pen-testing and training services. A multitude of attack modalities are already being developed and demonstrated within SHIELD, including Denial of Service, Data Exfiltration attacks etc.

- Using NFV products for cybersecurity awareness and defense: the SHIELD vNSFs will be added to the company's portfolio. An online store is envisioned to accommodate the new products and services stemming from the SHIELD cybersecurity vNSFs.
- Use of NFV products integrated in a SOAR pipeline: The easy deployment of NFV make them ideal candidates for a SOAR solution, providing that they can be easily integrated in a security team's workflow. Seamless control and configuration of VNF-based services can help establish the VNF ecosystem as a potential SOAR solution.

4.3.7. POLITO

POLITO is a major technical research university in Italy. The TORSEC cybersecurity group of the Department of Computer and Control Engineering at POLITO will exploit the outcomes of SHIELD in three main directions. For education, the results have already been (and will continue to be) used in courses at master level, to enrich the syllabus with advanced security topics, and as subject for MSc and PhD dissertations: we already had a couple of thesis related to the topics of SHIELD and more are under way. For research, the results will constitute the foundation for further proposals related to trust and security of SDN, NFV, and cloud infrastructures. In particular one proposal was submitted to a call on August 2018, it passed the threshold but unfortunately it was not funded. A new proposal is under way, related to the secure management of network infrastructures. Finally, for consultancy, the results of SHIELD have already permitted POLITO to offer better support to public bodies and private companies seeking advice about the improvement of their network infrastructure and the design of their security architecture. As an example, there are two regional projects (one already funded, and the other to be submitted on April 2019) that use some of the SHIELD technologies to protect industrial control systems. Last but not least, POLITO will jointly exploit some results with other partners: HPELB, POLITO, and TID plan to package and offer the Trust Monitor as a service for security-sensitive infrastructures. HPELB and POLITO have signed an agreement (valid beyond the end of SHIELD) to continue the development of a new virtual TPM and offer it to the TCG for potential inclusion in a future vTPM specification.

4.3.8. SPH

SPH is a telecom and IT value-added services provider, offering integrated telecommunications and IT solutions mostly to corporate customers in the financial, telco and public/defence sectors. SPH is already offering managed IT security services solutions, based on either on-site integrated equipment or on cloud SecaaS offerings. In the medium/long-term, SPH sees an important exploitation potential for the SHIELD solution as a whole, as a next-generation SecaaS solution which can be offered over NFV-enabled infrastructures. This can be developed in collaboration with the country's leading ISPs, which are already SPH customers. In the short term, a more directly exploitable result, which SPH is particularly focusing on, is the application of the DARE for advanced network insights, even for traditional (non-NFV-capable)

infrastructures. SPH intends to offer DARE as a complementary, cost-effective solution for traffic analytics and anomaly detection, to be deployed as an added-value service over integrated infrastructures (enterprise networks, data centre etc.). SPH expects that the DARE can be a significant source of revenue and profit as an add-on service, probably complementing commercially available SIEM solutions or even, in some cases, totally replacing them.

4.3.9. TALAIA

Talaia Networks is a highly innovative company based in Barcelona, Spain. Behind the products of Talaia Networks lies the expertise of more than 20 years of research in network security and monitoring from its founders at UPC-BarcelonaTech. The company aims to stay at the cutting edge of the state-of-the art in network management and security.

Talaia, the flagship product of Talaia Networks, is a network visibility and security system commercialized under the Software-as-a-Service model, that by combining machine learning and data analytics algorithms, obtains a superior security-to-cost ratio as compared to competing solutions. The interests of Talaia Networks lie in technologies for network security, key performance metric measurement, traffic classification, and on-the-fly streaming data analysis, enriched with intelligent machine learning algorithms, in both traditional and software-defined networks.

Talaia's exploitation plans include the adoption of VNF knowledge and technologies that will result from the SHIELD project and help accelerate Talaia's full integration with SDN architectures. Moreover, Talaia has a great interest in constantly evolving and enriching its anomaly detection engine with new types of cybersecurity threats and detection algorithms.

Talaia has already began the direct exploitation of the results of WP4 activities by introducing new capabilities to its application and anomaly detection engine, such as the detection of the Stratum protocol and cryptocurrency mining respectively. Furthermore, after Talaia's recent acquisition by Auvik Networks, the new features of its application and anomaly detection engines will gradually become commercially available to hundreds of MSPs, where the technologies and knowledge acquired from the SHIELD activities will be used in real scenarios on a daily basis.

4.3.10. TID

The Telefonica Group is one of the world-leading integrated operators in the telecommunications sector, with presence in Europe and Latin America. It operates in 21 countries. Telefonica's total number of customers amounted to 346 million[21]. In Europe, the Group has operations in Spain, the United Kingdom and Germany, providing services to more than 100 million customers at September 2017.

Telefonica Investigacion y Desarrollo (TID), as the branch of the Telefonica Group in charge of innovation and strategic vision, is in charge of researching emerging network and security technologies, as well as developing products and services based on them.

[21] https://www.telefonica.com/en/web/about_telefonica/in-brief

TID's exploitation plan will be comprised of several actions beyond the project lifetime, covering a wide range of topics from internal dissemination to technological transfers, to help business service deployment by Telefonica Business Units (BUs).

Knowledge and results transfer has been made during the project lifetime and will continue within Telefonica Data unit (LUCA), Telefonica cybersecurity Unit (11Paths) and different countries BU. The SHIELD frameworks model, and technical results, has been presented and discussed already. Furthermore, in the cybersecurity area a public webinar event[22] with Telefonica data unit (LUCA) was made. Also, TID did an internal workshop in the company with different global and Spain BU, including, service developments, marketing and operation. Details of the results will be depicted in D5.2.

TID's expectations is to continue in this path to leverage the SHIELD results as part of the variety of security services in design or already in production to enhance their capacity. Some examples are Managed Security Operations[23] service, Clean Pipes[24] product or "conexion Segura" service[25].

4.3.11. UBI

Ubiwhere is a Research and Innovation SME, based in Portugal, developing innovative and user-centered software solutions. As an SME focused on software development, Ubiwhere has been concentrating on two main areas: Telco & Future Internet as well as Smart Cities.

Since the foundation of Ubiwhere, the company has had a very strong interaction with biggest Portuguese communication companies (both ISPs and Vendors). Furthermore, Ubiwhere also has a close relation with regulators having in fact, currently in production, two national deployments for Portugal's national regulator (ANACOM). Ubiwhere has been actively researching for the last two years on NFV and SDN technologies with the aim to extend its commercial portfolio with a range of solutions based on these technologies. From the multiple contacts Ubiwhere has with communication companies (mainly in Portugal) it is clear that the path to use these kind of technologies is well established in their roadmap and so, Ubiwhere wishes to capitalize as soon as the need arises. In this context, Ubiwhere expects to extend its current network security portfolio with the vNSFs that are to be developed in the project.

Ubiwhere is currently a full ETSI member and is currently carefully following OSM development. Ubiwhere envisions the possibility of onboarding SHIELD's store component or at least some of its workflows in OSM solution. By doing this, Ubiwhere aims both at showcasing SHIELD's and Ubiwhere's research outcomes to potential partners/clients but also to have a considerable impact on how VNFs are onboarded in such an ecosystem. In this context, Ubiwhere showcased the vNSF package validation features within the ETSI OSM group. These presentations raised the interest from the ETSI OSM board with the possibility of integrating these features into the OSM solution ecosystem. Currently, the OSM board is analysing the implementation of

[22] https://www.eventbrite.com/e/luca-talk-6-redes-mas-seguras-con-machine-learning-tickets-35232602663 and https://www.youtube.com/watch?v=-e1knGuXKT8&t=16m30s

[23] https://www.elevenpaths.com/managed-security-operations

[24] https://www.elevenpaths.com/technology/clean-pipes

[25] https://www.telefonica.com/web/press-office/-/telefonica-offers-a-security-service-which-protects-the-connection-at-home-and-in-mobiles

SHIELD's package validation solution to check the feasibility of integrating it within the OSM product.

Network security analysis and mitigation component of SHIELD (DARE) is also of great interest to Ubiwhere. Both hardware and software attestations are features envisioned to be provided in the context of Ubiwhere's most recent product Smartlamppost[26]. The know-how, architectural design and software ecosystem is expected to leverage the implementation of such features in the context of Smartlamppost product.

[26] http://www.smartlamppost.com/

5. CONCLUSIONS

This Deliverable provided the final report on SHIELD exploitation activities including: recent updates of global cybersecurity market and environment; identification of SHIELD positioning in the market and its unique value proposition with its barriers; financial and economic analysis; as well as sensitivity and risk analysis in order to assess technology and market risks. Furthermore, strategic guidelines for the most appropriate services for development have been provided. In addition, joint exploitation plans and individual exploitation plans were identified.

From our analysis, it seems that still there does not exist a commercial and integrated solution offering both SOAR features and advanced mitigation capabilities tailored for virtual network services. The versatility of SHIELD is still acknowledged by the fact that offers capabilities of the other compared solutions, thanks to the distinctiveness of its architecture that allows for the synergy of different key components.

The techno-economic analysis quantified profitable business cases and opportunities for European players like operators with SMEs in the sector of NFV and Security Analytics via advanced innovative blend of services. The risk analysis showed that the investment in SHIELD by an established telco, will be able to yield a positive NPV in most of the cases.

Concluding, it can be deduced that the solution developed by SHIELD is very well positioned, given the market trends and evolutions, and exhibits a significant exploitation potential, both as an integrated platform as well as individual results.

REFERENCES

[1] Gartner Forecasts Worldwide Cloud-Based Security Services, available online http://www.gartner.com/newsroom/id/3744617

[2] Gartner Forecasts Worldwide Information Security Spending https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[3] Gartner's Market Trends: CSP Digital Transformation - Choosing the Right Path (oct 16)

[4] Ovum's "Defining the next-gen managed security services provider" (Ago 2017)

[5] Forrester Vendor Landscape: Global Managed Security Services, 2017

[6] AT&T - Managed Security Service. Product Assessment. Current Analysis (Nov. 2016)

[7] Forrester. The State Of Network Security: 2016 To 2017, Jan 2017

[8] Gartner, Critical Capabilities for Security Information and Event Management 2016

[9] Gartner, Magic Quadrant for Security Information and Event Management, 2016

[10] Eurostat Newsletter ICT usage in enterprises in 2018 193/2018 - 13 December 2018

[11] Cloud computing - statistics on the use by enterprises [online] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

[12] European Commission, Digital Single Market, Digital Agenda Scoreboard key indicators, available at: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators

[13] B. T. Olsen et al., "Technoeconomic Evaluation of the Major Telecommunication Investment Options for European Players", IEEE Network, vol. 20, no 4, July 2006.

[14] H. Attak (HPE), TPM performance improvement patch for Linux [online], https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9f3fc7bcddcb51234e23494531f93ab60475e1c3, Retrieved November 2017.

[15] Trusted Computing Group, SNMP MIB for TPM-Based Attestation https://trustedcomputinggroup.org/wp-content/uploads/TCG_SNMP_MIB_for_TPM-Based_Attestation_v0.8r2_PUBLIC_REVIEW.pdf

[16] K. Veeramachaneni, I. Arnaldo, A. Cuesta-Infante, V. Korrapati, C. Bassias, K. Li, AI 2: Training a big data machine to defend, 2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), 2016.

LIST OF ACRONYMS

Acronym	Meaning
AHP	Analytic Hierarchy Process
API	Application Programming Interface
ASAM	Advanced Security Analytics Module
BRAS	Broadband Access Server
CAPEX	Capital Expenditure
CERT	Computer Emergency Response Team
CISO	Cyber Incident Management & Security Operations:
C&C server	Command & Control server
CSP	Communication Service Provider
CR	Consistency Ratio
CRUD	Create, Read, Update, Delete (operations)
CVE	Common Vulnerabilities and Exposures
DAM	Data Access Manager
DARE	Data Analysis and Remediation Engine
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HDFS	Hadoop Distributed File System
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention System
IMA	Integrity Measurement Architecture
IRR	Internal Rate of Return
IoT	Internet of Things
IPS	Intrusion Prevention System

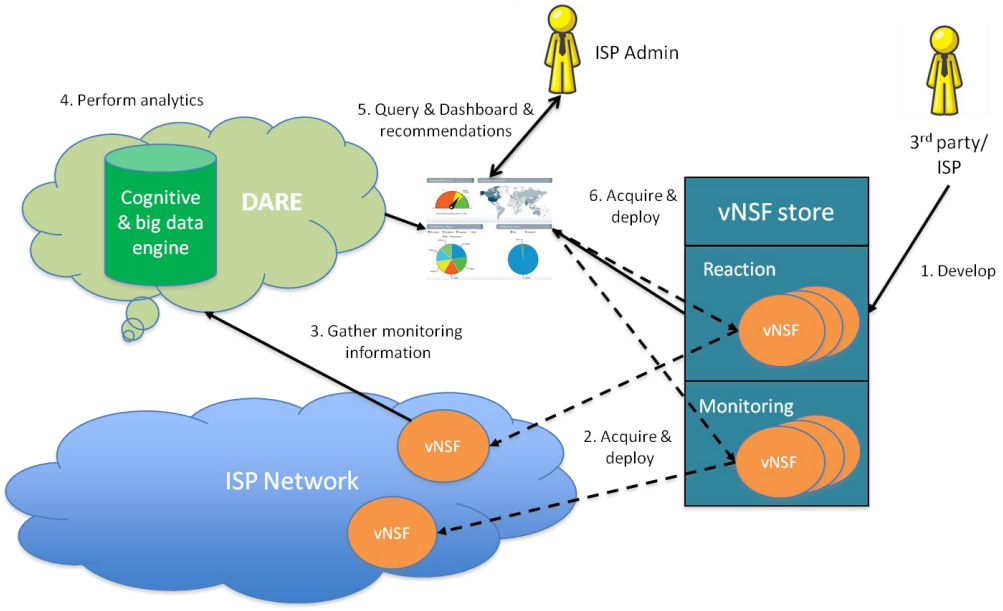
ISG	Industry Specification Group
ISP	Internet Service Provider
KPI	Key Performance Indicator
LDA	Linear Discriminant Analysis
LEM	Log & Event Manager
NGA	Next Generation Access
MANO	Management & Orchestration
MEC	Mobile Edge Computing
MSSP	Managed Service Providers
MSSP	Managed Security Service Providers
NGA	Next Generation Access
NF	Non-Functional (requirement)
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NPV	Net Present Value
NS	Network Service
OSSIM	Open Source Security Information and Event Management
OPEX	Operational expenditure
OTX	Open Threat Exchange
PaaS	Platform as a Service
PCI	Payment Card Industry
PCR	Platform Configuration Register
PF	Platform Functional (requirement)
PoP	Point of Presence
REST	Representational State Transfer
SAO	Security Automation and Orchestration
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

SOAR	Security Orchestration, Automation and Response
SOX	Sarbanes–Oxley Act
SP	Service Provider
STIX TAXII	Structured Threat Information Expression™ and Trusted Automated eXchange of Indicator Information
TC	Trusted Computing
TLM	Threat Lifecycle Management
TMaaS	Trust Monitoring as a Service
TSS	Telecom Security Service
TPM	Trusted Platform Module
UC	Use Case
uCPE	Universal Customer Premise Equipment
UI	User Interface
USM	Unified Security Management
vCPE	Virtual Customer Premise Equipment
VDU	Virtual Deployment Unit
vNSF	virtual Network Security Function
vNSFO	vNSF Orchestrator
vNSFD	vNSF Descriptor
VPN	Virtual Private Network
VSS	Virtualized Services Platform
WAF	Web Application Firewall
WACC	Weighted Average Cost of Capital

APPENDIX A. SHIELD USE CASES DESCRIPTION

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

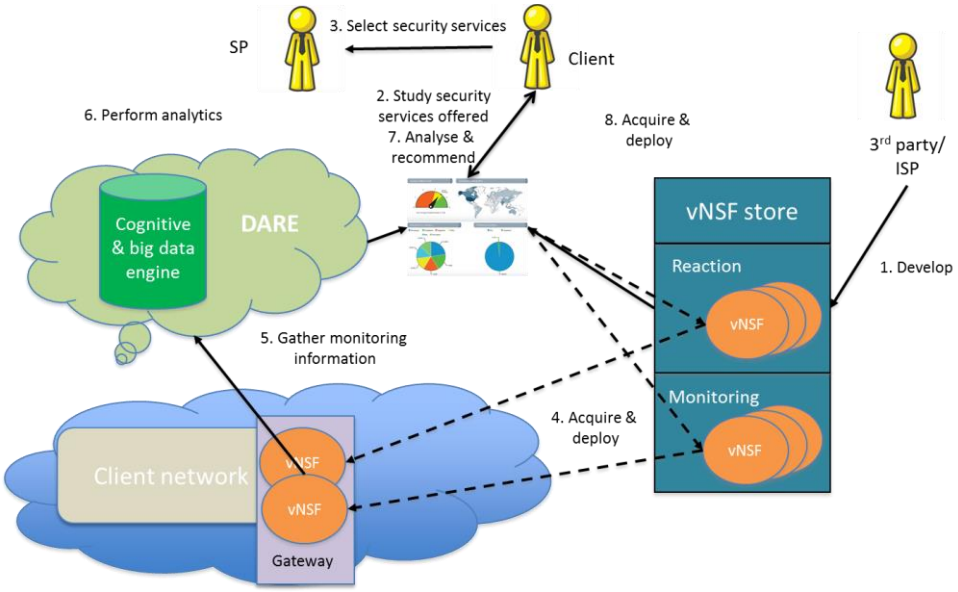
In order to protect their own network infrastructure, ISPs have to deploy specific hardware which is very expensive since this hardware has to be updated and maintained by very specialized operators. The virtualization offered by SHIELD in this use case aims to dramatically reduce this cost by replacing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