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

[H2020 - Grant Agreement No. 700199]

Deliverable D6.3

Interim 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), E. Trouva (NCSR Demokritos), O.E. Segou (Orion Innovations PC), A. Lioy, M. De Benedictis (Politecnico di Torino), G. Kolonias, T. Michalakis, G. Gardikis (Space Hellas S.A.), G. Dimopoulos (TALAIA Networks), A. Pastor, J. Núñez, (Telefonica I+D), T. Batista, R. Preto (Ubiwhere)

Version 1.0

Date November 30st, 2017

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 dedicated survey about the factors that influence the commercial success of the proposed technology has been conducted. All these findings have resulted in updated per-partner individual exploitation plans for the project results.

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. A more detailed requirements list of what should be expected in the market according to major consulting firms include: a shift from protecting the network to strategically protecting the business; coverage of new business opportunities; focus on prevention and detection rather than mitigation; as well as augmented detection capabilities using advanced machine learning algorithms, trained by security experts.

A market survey was conducted, analysing in brief the most dominant products and services in the field of cybersecurity, focusing on SIEM platforms and virtualised services on the cloud. The versatility of SHIELD is acknowledged 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 SIEM features and advanced mitigation capabilities focused on virtual network services. In this respect, SHIELD manages to organically link advanced SIEM and big data analytics with virtual/software network domain. Easy deployment of network services and integration with DARE's SIEM capabilities is expected to be a key innovation of SHIELD, filling a specific market need, especially in the context of future/5G networks, which will be software-based.

SHIELD is indeed a newcomer on an extremely competitive market, populated mostly by companies that are pioneers in the cybersecurity domain. SHIELD has to overcome a few major barriers like the trust on the vendor, vendor lock in, market positioning and usability issues. Furthermore, a SWOT analysis oriented to Managed Security Services Providers (MSSP) illustrates that NFV needs to constitute a key technology driver for future MSS. In open NFV-based solutions such as SHIELD, there is a clear risk in the lack of virtual security appliance offerings, if there is no involvement of vNSF security vendors (vNSF developers). Moreover, a lack of cyber threats feeds (e.g. network dumps from actual incidents) in order to train the detection algorithms in the DARE should be addressed. It also seems that, bringing mechanisms such as remote attestation from the research field to a commercial NFV solution is a clear differentiating factor to be prioritized for solutions such as SHIELD.

In order to better steer the further development of the system during Y2 and set priorities, the SHIELD consortium launched a survey, focusing on the factors that will affect market adoption

and evolution of the SHIELD solution. Apart from the traditional method of collecting experts' opinions, the survey uses the Fuzzy Analytic Hierarchy Process (FAHP) methodology for the Criteria Comparison Part. The online survey was addressed at targeted persons, both within and outside the consortium, that are professionally engaged with information security tasks. It was divided in two parts: profiling of the experts and comparison of criteria. A multi-level hierarchy of criteria was constructed, consisting of three levels (the objective under investigation -that is, the factors that will affect market adoption and evolution of SHIELD solution- the individual criteria, affecting the objective, and, finally their relevant sub-criteria, each of which represents a specific feature/characteristic.

According to the survey results, the criterion that is the most important one to take into account is that of "Performance"; the market needs performant solutions which can cope with vast amounts of data under minimal response time. Taking this into account, it can be deduced that the performance KPIs need to be reached independently of the underlying technology.

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

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

All the above mentioned conclusions, as well as the lessons learnt from the Y1 activities, helped the SHIELD partners to update their exploitation plan and better position their ambition with respect to the project results.

Table of Contents

1. INTRODUCTION 6
2. SHIELD POSITIONING IN THE MARKET 7
2.1.1. Evolution of the market 7
2.1.2. Possible competitors 8
2.1.3. Description of Competitors 9
2.1.3.1. AlienVault Unified Security Management (USM) & OSSIM 9
2.1.3.2. ArcadiaData 10
2.1.3.3. BlackStratus cybersecurity solutions 10
2.1.3.4. Cisco Umbrella 11
2.1.3.5. EMC (RSA) NetWitness Suite 12
2.1.3.6. EventTracker 13
2.1.3.7. FortiSIEM (Fortinet) 14
2.1.3.8. Fortinet Next Generation Firewall (Fortigate NGFW) 15
2.1.3.9. IBM Security QRadar 16
2.1.3.10. LogRhythm Security Intelligence and Analytics Platform 16
2.1.3.11. ManageEngine 18
2.1.3.12. RAD vCPE Toolbox 18
2.1.3.13. SolarWinds 20
2.1.3.14. Splunk Enterprise 20
2.1.3.15. VSS of Nuage Networks (Nokia) 22
2.1.4. Product Comparison 24
2.1.5. Barriers for SHIELD 29
2.1.6. SWOT Analysis 30
3. SHIELD ROADMAPPING 33
3.1. Roadmapping Criteria and Method 33
3.2. Evaluation Results and Discussion 39
3.2.1. Weighting of each criterion 39
3.2.2. Weighting of Sub-criteria under each criterion 43
3.2.3. Global priorities of sub-criteria 46
4. INDIVIDUAL EXPLOITATION PLANS 48
4.1. HPELB 48
4.2. I2CAT 48

4.3. inCITES 49
4.4. INFILI 49
4.5. NCSRD 49
4.6. ORION 50
4.7. POLITO 51
4.8. SPH 51
4.9. TALAIA 51
4.10. TID 52
4.11. UBI 52
5. CONCLUSIONS 54
REFERENCES 55
LIST OF ACRONYMS 56
APPENDIX A. SURVEY QUESTIONNAIRE 59
SHIELD in a nutshell 59
Methodology 60
Questions 61
Profiling 62
Criteria 62
Importance of the Technology Enablers 63
Importance of the SIEM-like functionalities 64
Importance of the Platform Features 64
Importance of the Performance 65
Importance of the Business /Strategy aspects 65
Importance of the Ease of Use 66
Use Cases description 66

1. INTRODUCTION

This Deliverable provides an initial report on SHIELD exploitation activities including: analysis of global cybersecurity market and environment, identification of SHIELD positioning in the market and its unique value proposition. This deliverable also demonstrates the barriers that may limit system's development. Furthermore, the factors that influence the success of the proposed technology 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 D6.3 addresses the first two points.

This document is organised in three sections: in the first section, the SHIELD position 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 a SWOT analysis, are presented. In the second part, a detailed Roadmapping analysis identifies the factors that will affect market adoption and evolution of SHIELD solution. In the last part, the updated per-partner exploitation plans and results in addition to the global initial exploitation results are illustrated.

2. SHIELD POSITIONING IN THE MARKET

2.1.1. Evolution of the market

Growth in worldwide cloud-based security services will remain strong, reaching $5.9 billion in 2017, up 21 percent from 2016, according to Gartner, Inc. The overall growth in the cloud-based security services market is above that 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 are expected to double and be more than $107B in 2017[3]. These services will have an annual growth rate (CAGR) of 23.5%. By 2017, Software-as-a-Service will remain the largest public IT services category, capturing 59.7% of revenues in

[1] http://www.gartner.com/newsroom/id/3744617
[2] http://www.marketsandmarkets.com/PressReleases/penetration-testing.asp
[3] https://softwarestrategiesblog.com/tag/cloud-computing-forecasts/

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 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 offers and basic management. The next evolutionary step in the market will be offer End-to-end Security Solutions. Gartner [2] predicts that these 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 ranked to cover these CSP needs.

A more detailed requirements list of what should be expected in the market according to Ovum [3] and Forrester [4] 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.

2.1.2. Possible competitors

This subsection provides an overview of products and services (in alphabetic order) similar to SHIELD that 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. 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 SIEM capabilities and the advanced mitigation capabilities of virtual 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 a specific market need.

2.1.3. Description of Competitors

2.1.3.1. AlienVault Unified Security Management (USM) & OSSIM

Description:

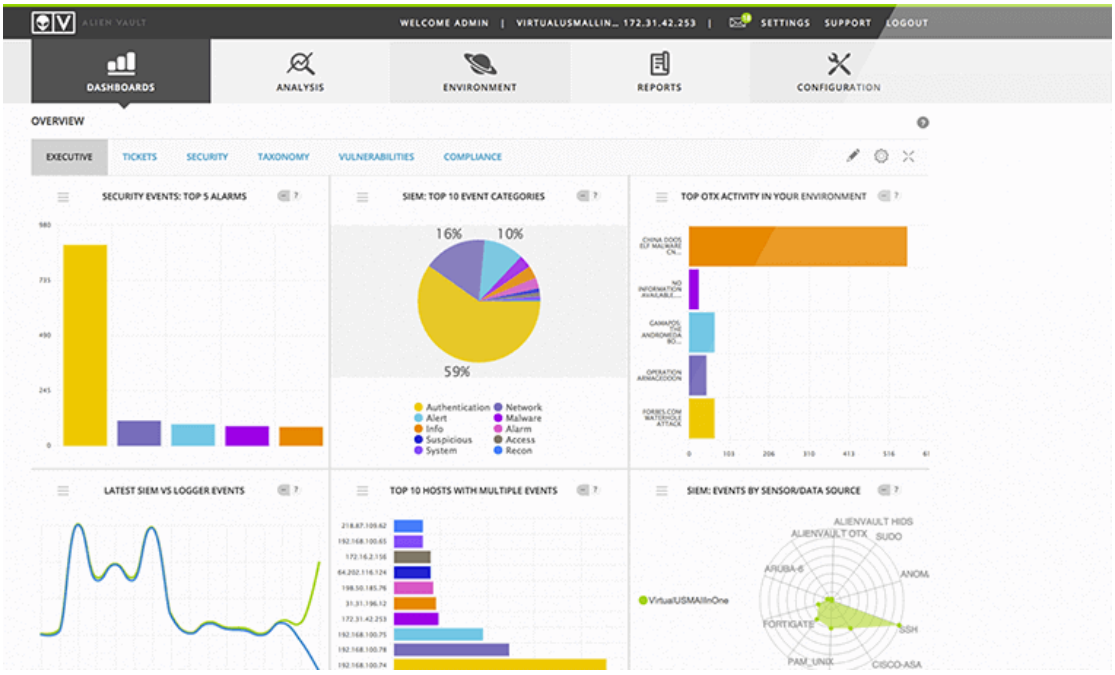
AlienVault's Unified Security Management[4] consists of five core capabilities:

- **Asset Discovery** allows the client to catalogue and monitor all assets in their network.
- **Behavioral Monitoring** identifies suspicious behavior and potentially compromised systems.
- **Vulnerability Assessment** scans environments to detect vulnerabilities and offer remediation recommendations.
- **SIEM** correlates and analyses security events across the environment (cloud or network)
- **Intrusion Detection** inspects traffic between devices and assets for anomalies related to intrusions, data exfiltration etc.

The solution is available for an on-premise deployment or cloud-based deployment. AlienVault allows certified third party organisations to offer USM as-a-Service to their clients.

Threat data are exchanged with AlienVault Labs Security Research Team and reported in Open Threat Exchange™ (OTX™) format and shared with the AlienVault open community. Logging is also compliant with PCI, HIPAA, and SOX.

Open Source Security Information and Event Management (OSSIM) is an Open Source version of USM is available through AlienVault's website. OSSIM offers the same basic core capabilities, excluding Log Management, Compliance checking, Automatic Threat Updates, Deployment & Support etc.



[4] https://www.alienvault.com/products

Figure 1. AlienVault USM, offered as a cloud-based service or installed on-premises.

Comparison with SHIELD:

Similar to USM, SHIELD is also designed to offer multiple deployment options (on-premises, cloud-based, or offered as-a-Service). SHIELD further introduces collection of data from SDN/NFV, while also ensuring ETSI-compliance and trusted computing through attestation of SDN/NFV components. The flexibility in defining NFV topologies makes SHIELD more adaptable to modern threats and multi-vector cyberattacks. Compliance with PCI, ISO can be foreseen, while HIPAA and SOX are not currently considered as they are US-specific.

2.1.3.2. ArcadiaData

Description:

Arcadia[5] Data offers cybersecurity visual analytics either to customers who have already built their own cybersecurity platform or to customers seeking to build a new one. For this reason, the company does not offer a novel security solution but is instead based on the Apache Spot cybersecurity framework that runs on the Cloudera Enterprise Data Hub. Being in close collaboration with the Spot community, Arcadia Data has provided contributions to the Open Data Model script that enables the building of directories and tables from specific sources to fit the Apache Spot ODM schema and three new dashboards focused on tracking and exploring security events related to users, endpoints, and vulnerabilities.

Comparison with SHIELD:

SHIELD's Cognitive Data Analysis module which is one of the two cybersecurity engines leveraged for anomaly detection and response is also based on the open-source Apache Spot framework, whose capabilities will be expanded to fulfil the project's needs. At the same time, the Security Data Analysis module offers an additional mature network monitoring solution, based on big data and machine learning in a SaaS package that provides actionable intelligence and executes metadata retention policies. The two modules are based on different analytics techniques and are working in parallel, aiming to provide a unified advanced security output.

2.1.3.3. BlackStratus cybersecurity solutions

Description:

BlackStratus[6] offers three products for cybersecurity awareness:

- SIEMStorm™ is a SIEM solution that incorporates data across devices, applications and databases, threat visualization and mitigation tools, built in the workflow.
- LogStorm™ is a log management tool that allows correlation between logged security events and prioritization in the reporting of threats to be mitigated
- CYBERShark™ is a Security as-a-Service offering that combines SIEM, log management and compliance checking, in the cloud.

[5] https://www.arcadiadata.com/solutions/cyber-security/
[6] https://www.blackstratus.com/

SIEMStorm™ main features include visibility across devices, applications and databases. It is installed on-premises as a single appliance that offers: regulatory compliance and business continuity, multitenancy support, real time visualization of attacks including zero-day vulnerabilities (with rules-based, vulnerability, statistical and historical correlations – including CVE compliant vulnerability intrusion detection), and reporting compliant with CPI, HIPAA, ISO, SOX.

LOGStorm™ is a log management and log monitoring solution, deployed on-premises as an appliance. It combines log management with real-time event log correlation and log monitoring, and integrates incident response. The main features of LOGStorm™ include: real time visibility, compliant and auditable log management, on-board storage prioritized threat identification, alerting and remediation guidance.

CYBERShark™ offers the BlackStratus security and compliance platform as-a-Service to its customers, without the need to deploy separate appliances. CYBERShark is especially marketed as a low-cost solution for SMEs and businesses that require a low-cost cybersecurity investment.

Figure 2. BlackStratus SIEM environment.

Comparison with SHIELD:

Similar to BlackStratus, SHIELD is designed to be offered on-premises, and as-a-Service. SHIELD also includes data collected from SDN/NFV. As SDN deployments become more mainstream, this is a significant advantage for SHIELD. SHIELD's solution can be more flexible and adapt to threats with differing NFV topologies, while also maintaining ETSI-compliance. In terms of log management, SHIELD is not yet as mature as BlackStratus although CPI and ISO compliance is considered. HIPAA and SOX compliance are US-specific and are not considered at the moment.

2.1.3.4. Cisco Umbrella

Description:

Cisco Umbrella[7] is a purely cloud-based security solution and mostly relies on deploying secure internet gateways in the cloud. It is particularly appropriate for enterprises with distributed workforces, involving mobile employees working over VPN or directly with the cloud.

The main features of the Umbrella platform are:

DNS & IP layer enforcement: Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections.

Intelligent proxy: Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection.

Command & control callback blocking: Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers.

Visibility outside the perimeter: Umbrella provides visibility into internet activity across all devices, over all ports, even when users are off the corporate network. The logs can be retained forever.

Statistical models: Umbrella analyzes data to identify patterns, detect anomalies and create models to predict if a domain or IP is likely malicious. It automatically correlates data and blocks attacks.

Browser-based interface: The Umbrella dashboard provides both central and local administration and reporting.

Umbrella comes in three different service packages, in order to suit the needs of small, medium and large enterprises respectively.

Comparison with SHIELD:

Just like SHIELD, Umbrella uses the power of virtualization and the cloud in order to deploy SecaaS services instantly with minimal configuration effort. Unlike SHIELD SecaaS, which requires an NFV-enabled infrastructure, Umbrella works with today's network technology. However, NFV-based security has some profound advantages; first, it is deployed in the network, so it's easier to mitigate distributed attackes; and, second, it has significantly less delay due to the proximity of the virtual appliances to the endpoints. Also, the SHIELD platform can also be installed on-premises, which is quite important for organisations which, for policy reasons, do not want to offload security services to the cloud.

2.1.3.5. EMC (RSA) NetWitness Suite

Description:

NetWitness[8] is RSA's (now EMC) suite for advanced threat detection and cyber incident response. NetWitness offers as main features:

Advanced threat protection: NetWitness collects data across more capture points (packets, logs, endpoints, NetFlow, threat intelligence) and compute platforms (physical, virtual, cloud) than other solutions. Next, it applies a combination of behavior analytics, data science

[7] https://umbrella.cisco.com/
[8] https://www.rsa.com/en-us/products/threat-detection-and-response

techniques and machine learning algorithms to baseline "normal" network and endpoint behavior, identify attack indicators and minimize false positives.

Network monitoring and forensics: Raw data is parsed into metadata and sessionized at capture time to support security analytics and event reconstruction.

Endpoint security: NetWitness delivers visibility into processes, executables, events, and behavior on all the endpoints in the infrastructure (servers, desktops, laptops, virtual machines). "Alert fatigue" is alleviated by flagging suspicious modules and endpoints, prioritizing the threats according to an intelligent, automated risk-scoring algorithm and providing a clear visual indication of each endpoint's threat level. The platform scales easily from hundreds to hundreds of thousands of endpoints. Its workflow engine aligns with industry standards from NIST, US-CERT, SANS and VERIS.

Behavioural analytics: The platform detects both the "covert channels" attackers use to deliver malware to victims as well as communication between command-and-control (C2) sites and compromised hosts. This helps security teams spot advanced persistent threats earlier in the attack cycle.

Cyber Incident Management & Security Operations: NetWitness presents incident data, investigations and reports in multiple formats that security teams can customize by role or function (analyst, incident responder, security operations center manager, CISO) to match their workflows.

Comparison with SHIELD:

Apparently, the NetWitness platform has very similar scope with the SHIELD DARE, especially due to the fact that, like DARE, it does not rely on specific rules and heuristics to detect threats, but it employs (mostly statistical-based) anomaly detection approaches. NetWitness also incorporates workflow management and endpoint monitoring, which are not core objectives for SHIELD. It is also a complete commercial platform, with many data sources, algorithms and options to choose from. On the other hand, SHIELD emphasizes openness, providing support for third-party services and algorithms and also features integration with NFV environments (and thus support for highly dynamic and reconfigurable network services).

2.1.3.6. EventTracker

Description:

EventTracker SIEM[9] is a comprehensive security platform that delivers advanced security tools with audit-ready compliance capabilities. It offers a wide range of security essentials from endpoint threat detection to behavioural correlation. It comprises of 5 main capabilities:

- SIEM and Log Management as-a-Service that includes real-time alerting and incident response, prioritization of operational incidents and co-management of the platform with the company's analyst team.
- Signature-based threat Detection and Response from both internal and external sources based on incorporation from STIX/TAXII-compliant providers and other commercial and open source threat feeds and integration of an IDS system.

[9] https://www.eventtracker.com/solutions/siem/

- Vulnerability Assessment as-a-Service, regarding network malicious behaviour managed by the company's staff in order to reduce false positives.
- Entity Behaviour Analytics leveraging machine learning capabilities for the detection of abnormal user or entity behaviour.
- Automation of the steps required for compliance to several security standards.

Comparison with SHIELD:

SHIELD also offers an as-a-Service deployment option by leveraging SDN/NFV components and can thus be applied to a wider range of use-cases, such as the monitoring of ISP traffic, without being limited to enterprise environments. Due to the use of Big Data and distributed computing technologies, SHIELD offers a more scalable security infrastructure. The integration of two parallel cybersecurity engines based on machine learning as well as the implementation of remediation policies make SHIELD a more versatile solution against zero-day exploits that are typically not being detected by signature-based systems. SHIELD also offers behaviour analytics and real-time monitoring and alerting and is ETSI-compliant.

2.1.3.7. FortiSIEM (Fortinet)

Description:

From the product datasheet[10]: "*FortiSIEM provides organizations with a comprehensive, holistic and scalable solution, from IoT to the Cloud, with patented analytics that are actionable to tightly manage network security, performance and compliance standards, all delivered through a single pane of glass view of the organization. Fortinet has developed an architecture that enables unified and cross-correlated analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the threat data available in the organization. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for handling real-time searches, rules, dashboards and ad-hoc queries.*"

FortiSIEM was added to the Fortinet portfolio with the acquisition of accelops in 2016, it provides organizations a high level of functionality and has an intuitive dashboard that allows the operator to quickly and easily respond to a perceived threat. With this purchase, Fortinet entered the SIEM market with a mature product and established itself as a true competitor to the bigger companies in the market.

[10] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf

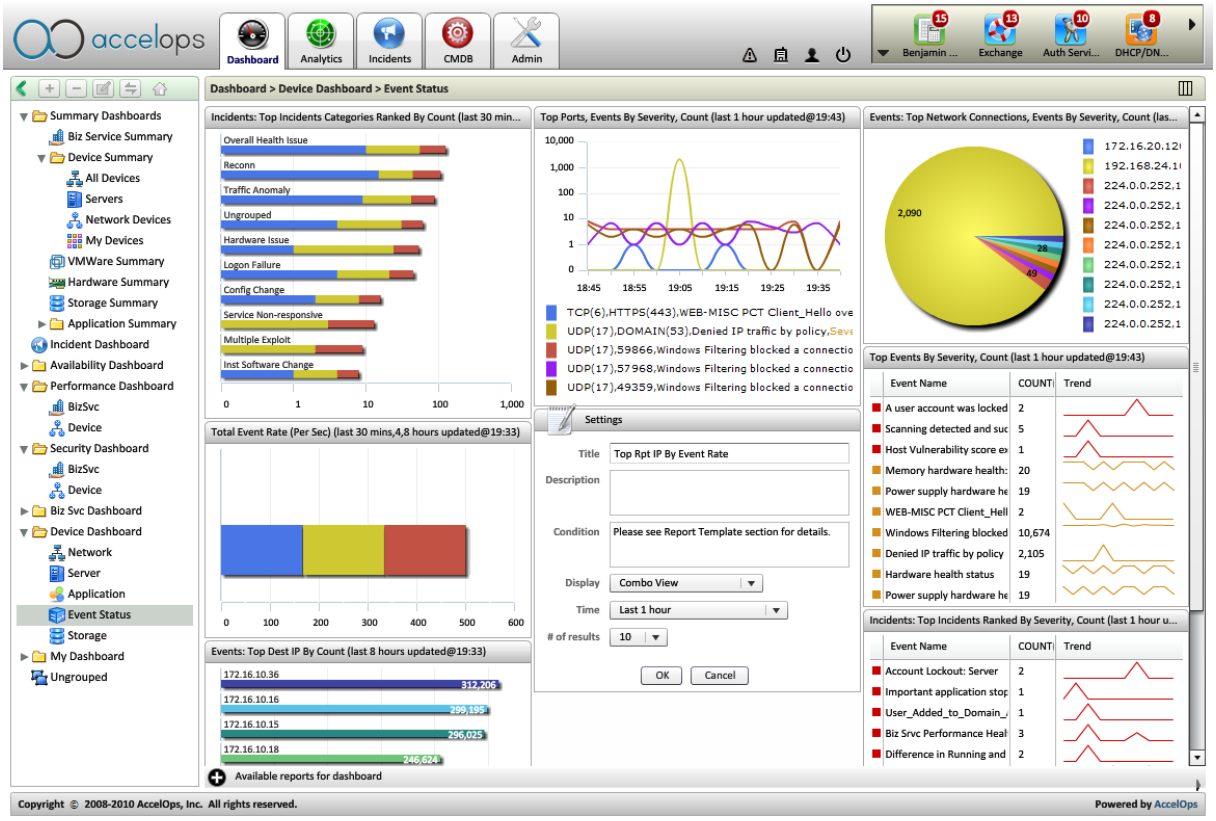


Figure 3 Fortinet (accelops) dashboard

Comparison with SHIELD:

FortiSIEM is a traditional SIEM. Its engine correlates events coming from a wide array of sources and searches for known anomalies on those patterns. This has the advantage of allowing for a very low rate of false positives, as the engine can be fine-tuned to search for specific events. It is able to use existing systems as data sources, including network analysis tools.

SHIELD is primarily a network traffic analysis tool. It will not try to perform any analysis of the end user systems. On the other hand, SHIELD can take advantage of its multiple analysis methodologies to detect both known and emerging threats before other solutions. FortiSIEM has one advantage over SHIELD, its varied data sources, on the other hand, SHIELD has the potential to detect threats that FortiSIEM would not detect, and offer automatic mitigation for many of those threats, lowering the barrier to entry for non-expert users.

2.1.3.8. Fortinet Next Generation Firewall (Fortigate NGFW)

Description:

This product[11] is not a full-fledged SIEM product, but an advanced firewall with IPS capabilities. Its only data source is the network traffic that crosses its domain. It has SSL inspection capabilities via “man in the middle”, and performs exceedingly well against known threats. This product is well integrated with Fortinet’s Unified Threat Management system, where it acts as

[11] https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-firewall/next-generation-firewall-ngfw.html

one of the policy enforcers. As a standalone product, it can be compared with IPS solutions like Suricata or Snort.

Comparison with SHIELD

Given the large functionality overlap between Fortinet's NGFW and a product like Snort, and given that Snort acts as one of SHIELD's information source, NGFW could in theory fulfill the same role. Given that it (unlike Snort or Suricata) comes pre-configured with a very useful set of rules, its IPS features could be used on shield as a mitigation for known threats, potentially alleviating some of the work performed by SHIELD's Machine Learning engines that are able to detect potentially new threats (0-day) due to the difference in traffic patterns.

2.1.3.9. IBM Security QRadar

Description:

QRadar[12] is the leading SIEM solution from IBM and one of the most well-known in the market. QRadar aims at providing timely notifications about anomalies in the infrastructure, while keeping false positives to a minimum.

To achieve this, QRadar first collects and consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. Then, it then uses an analytics engine to normalize and correlate this data and identifies security offenses requiring investigation. QRadar reduces and prioritizes alerts by focusing security analyst investigations on a short, manageable list of suspected, high probability incidents. It also complies with internal organizational policies and external regulations by offering many customizable reports and templates.

Comparison with SHIELD:

QRadar uses massive analytics on heterogeneous data sources in order to infer anomalies, which is a functionality very similar to DARE, to which there are seemingly a lot of common features. QRadar (such as the SHIELD DARE) supports scaling up just by adding compute/storage nodes and also supports extension by plug-in security services (from the IBM Security App Exchange). It also features an intuitive reporting engine, whereas high customization of reports is not well within SHIELD scope. On the other hand, the DARE supports extension by third-party algorithms and services and also integrates with NFV environments for automatic mitigation.

2.1.3.10. LogRhythm Security Intelligence and Analytics Platform

Description:

LogRhythm[13] sells its SIEM solutions to midsize and large enterprises. LogRhythm's SIEM can be deployed as an appliance, software or virtual instances and supports an N-tier scalable, decentralized architecture composed of the Platform manager, AI Engine, Data Processors, Data Indexers and Data Collectors. Consolidated all-in-one deployments are also possible. System Monitors and LogRhythm Network Monitor can optionally be deployed to provide

[12] https://www.ibm.com/us-en/marketplace/ibm-qradar-siem
[13] https://logrhythm.com

endpoint and network forensic capabilities, such as system process, file integrity and NetFlow monitoring, deep packet inspection (DPI) and full packet capture. LogRhythm combines event, endpoint and network monitoring capabilities with UEBA features, an integrated incident response workflow and automated response capabilities. LogRhythm CloudAI offers Security Analytics Enabled by AI and as the fully integrated add-on for the LogRhythm TLM Platform, provides a holistic view to accurately accelerate threat qualification and remediation against user, endpoint, and network threats. CloudAI gives offers accuracy by using AI and machine learning to detect signature-less and hidden threats.

Concerning Real-Time Monitoring, LogRhythm provides more than 900 out-of-the-box correlation and detection rules, with additional modules focusing on specific use cases or verticals and offers a dashboard (customizable) presenting a real-time threat map and other widgets provides analysts with an overview of threat activity. Network Monitor adds network traffic monitoring and forensic capabilities and allows correlation with log-based sources.

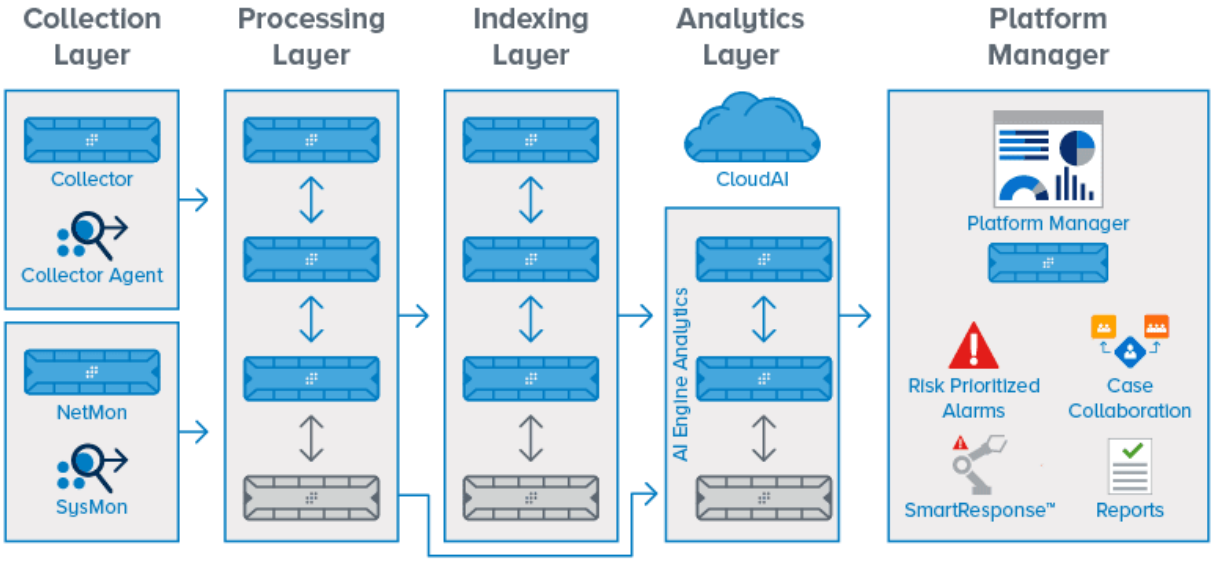


Figure 4. LogRhythm - Threat Lifecycle Management

LogRhythm network monitoring solution approach covering the endpoint, payload and network layers. DPI and endpoint monitoring are seamlessly integrated with the SIEM. In addition, they offer the Honeypot Analytics Suite (open-source honeypots that can be used to aid in threat hunting). A number of third-party integrations are also supported, including Symantec, McAfee, FireEye, Bromium and Carbon Black.

LogRhythm's User Threat Detection Module is available as an additional component and provides machine-learning-based UBA capabilities. LogRhythm can directly monitor database audit logs, and there is integration with third-party DAM technologies.

Behavioral profiling and anomaly detection are supported across a variety of attributes obtained from event, log and endpoint sources, as well as network activity based on flows and DPI. The LogRhythm User Interface has been developed in HTML5 and requires no additional plug-ins. The LogRhythm Deployment manager, used to manage the LogRhythm system architecture, is provided as a fat client.

Horizontal and vertical scaling and distributed deployment are supported. LogRhythm can be deployed as an appliance, software, virtual image and infrastructure as a service (IaaS) on Amazon AWS and Microsoft Azure. System Monitor Agents are available for Windows, Linux and Unix.

Security Automation and Orchestration (SAO) functionality alleviates security team fatigue through expedited and automated workflows that accelerate threat qualification, investigation, and response to a variety of different use cases. LogRhythm's Elasticsearch indexing layer and big data analytics platform allows the finding of relevant information quickly.

Comparison with SHIELD:

LogRhythm like other SIEM vendors is pivoting toward SA by adding NAV (Network Analysis and Visibility) and Security User Behavior Analytics (SUBA) capabilities to their existing solutions SHIELD is more focused to resource optimization, providing security intelligence in a centralized node (DARE) and supporting 3rd party vNSFs to add monitoring or mitigation capabilities.

2.1.3.11. ManageEngine

Description:

ManageEngine's[14] Advanced Security Analytics Module (ASAM) is a network flow based security analytics and anomaly detection tool that helps in detecting zero-day network intrusions, using the state-of-the-art machine learning technologies, and classifying the intrusions to tackle network security threats in real time. ASAM offers actionable intelligence to detect a broad spectrum of external and internal security threats as well as continuous overall assessment of network security.

The Security Snapshot of ASAM displays a list of grouped threats/anomalies as problems and further, the problems are categorized in to three major problem classes (Bad Src-Dst, DDoS, Suspect Flows). The set of classes used for classifying problems with a brief description is given here (Problem Taxonomy). The pie charts and line graphs help the user grasp the overall network "security posture" in one glance. On further drill-down it displays a list of individual events/anomalies, of a specific problem, with detailed information collation for closer investigation by the operator.

Comparison with SHIELD:

Similar to SHIELD, ASAM leverages state-of-the-art machine learning algorithms to detect and classify anomalies. However, it lacks some of SHIELD's most notable features, i.e. automated mitigation strategies against the detected security threats.

2.1.3.12. RAD vCPE Toolbox

Description:

[14] https://www.manageengine.com/products/netflow/network-behavior-analysis-using-advanced-security-analytics-module.html

RAD[15] is a global Telecom Access solutions and products vendor. Through its vCPE (virtual Customer Premise Equipment) Toolbox provides the basis to deploy virtualized security services to customers.

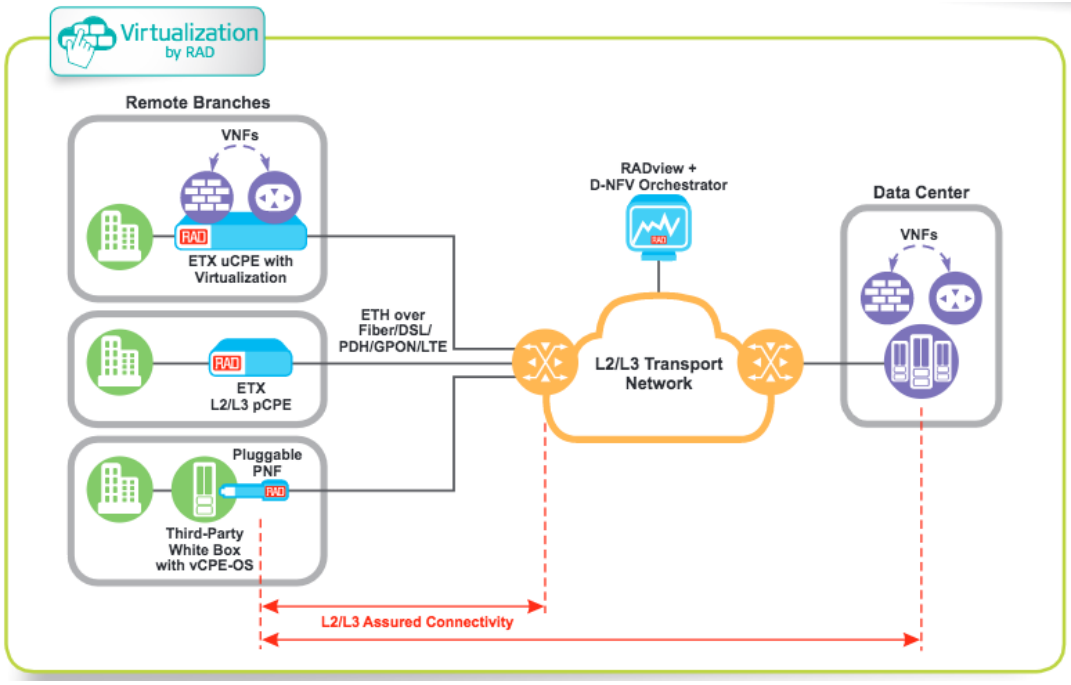


Figure 5. RAD Virtualization vision

RAD provides a range of vCPEs to fit the different types of customer edge requirements. The platform is an open platform and it is able to deploy any VNF available over x86 architecture running in KVM hypervisor technology.

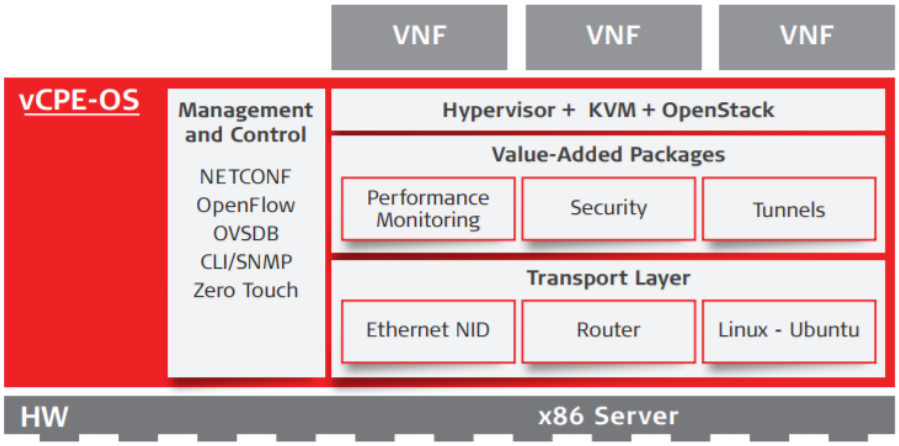


Figure 6. RAD vCPE architecture

The NFV lifecycle management is provided in collaboration with the Amdocs company.

The security service is directly provided by the vNSF deployed in the vCPE and provided by third parties (VNF). There is not a security solution provided by RAD itself.

[15] http://www.rad.com/14/vCPE/35976/

Comparison with SHIELD:

RAD covers the Use Case 2 providing security services to enterprise customers. It provides a NFV infrastructure with specific user equipment (vCPE) to deploy VNFs (vNSFs in SHIELD terminology) from third parties acquired by the user. RAD provide a solution very similar to SHIELD concept but the key difference is that SHIELD is also offering security intelligence in a centralized node (DARE). In this way SHIELD allows the deployment of professional security solutions, allowing vNSFs to be less complex and with less resource requirements, since security decisions are taken by the DARE and not by the vNSFs. Also, the remote service attestation capability offered by SHIELD is limited to VNF integrity on boot process.

2.1.3.13. SolarWinds

Description:

The SolarWinds SIEM Log & Event Manager (LEM)[16] is a solution for log management, forensic analysis, compliance and troubleshooting. LEM collects and analyses logs, correlates important events to identify threats and takes automatic action to defend against them.

More specifically, the threat intelligence feed inspects for matches against known bad hosts and other threats and provides information that is used to create Active Responses that represent the logic to trigger an alert or an automated mitigation action. An active response can be an automated action to block IPs, stop services, disable users and more.

Comparison with SHIELD:

Similar to SHIELD, SolarWinds' LEM offers users a set of recommended rules, tailored to match the characteristics of different types of threats. The selected recommendation rules are in turn converted mitigation actions which can be applied in a manual or automated fashion.

In contrast to SHIELD which supports on-premises or cloud-based deployment options, LEM is only offered as an on-premises deployment. This has direct impact on the product's flexibility and scalability.

2.1.3.14. Splunk Enterprise

Description:

The Splunk[17] Security Intelligence platform is composed of Splunk Enterprise, the core product that provides event and log collection, search and visualization, Splunk for Enterprise Security and Splunk UBA. Data collection and analysis is the primary feature of Splunk Enterprise. Splunk Enterprise Security provides predefined dashboards, correlation rules, searches, visualizations, workflow and reports to support real-time security monitoring and alerting, as well as compliance reporting use cases. Splunk Enterprise and Enterprise Security can be deployed on-premises, in public or private clouds, or as hybrid configurations. Splunk Enterprise and Splunk Enterprise Security are also available as SaaS offerings (Splunk Cloud, Splunk ES Cloud). This document assesses critical capabilities for Splunk Enterprise in combination with Splunk for Enterprise Security.

[16] https://www.solarwinds.com/log-event-manager
[17] https://www.splunk.com/en_us/products/splunk-enterprise.html

Splunk Enterprise Security includes predefined mapping for security event sources, security-specific correlation searches, reporting and security monitoring dashboards for real time monitoring. Workflow allows incident management leveraging features, such as the Investigator Journal and Investigation Timeline, includes integration with third-party applications. Integration with popular third-party service desk solutions and services is provided.

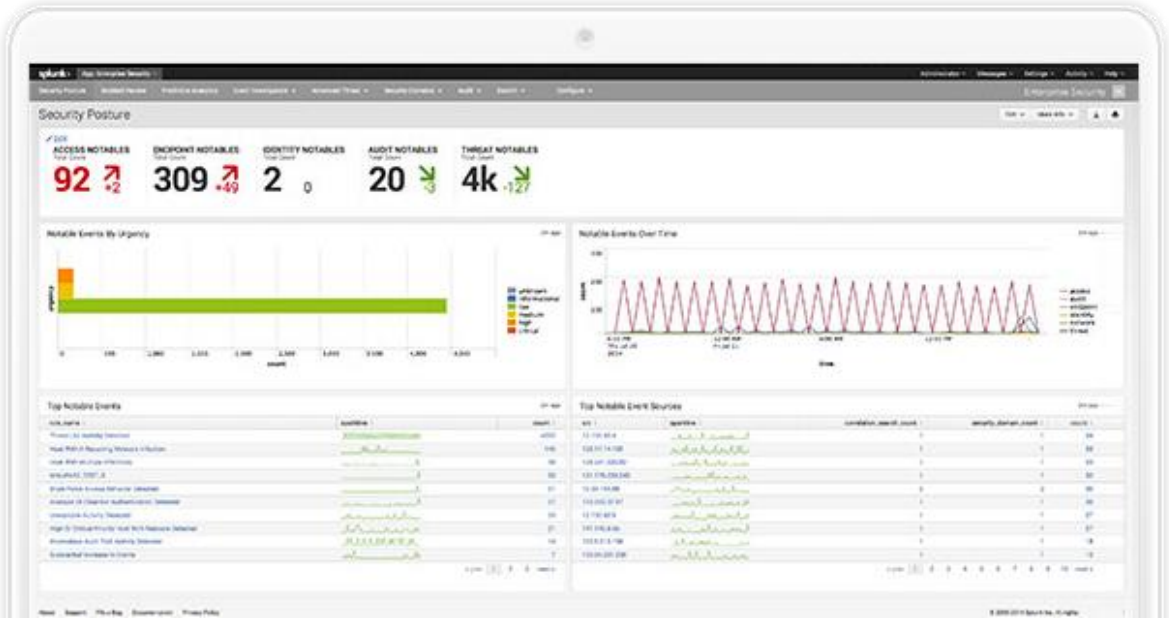


Figure 7. Splunk - Security Posture Dashboard

Splunk uses a combination of approaches (machine learning, statistics and rules) to discover anomalous activity that could be symptomatic of advanced threats. Additionally, advanced analytics and threat modeling is used to detect advanced threats across different vectors, such as email, malware and web-based attacks. Splunk App for Stream analyzes wire data including HTTP, DNS communications in real time to provide network visibility, which can be correlated with additional data. The deployment of Splunk is based on Big Data Architecture – Slave and Master.

Splunk Enterprise Security provides a threat intelligence framework that allows users to acquire and aggregate internal and external threat sources, including support for STIX/TAXII and Open IOC. Splunk also provides identity-oriented monitoring for enterprise cloud SaaS applications, via partnerships with SaaS vendors, such as Box and Salesforce. Splunk provides native user and entity behavior modeling via the Splunk UBA product. Splunk provides compliance that address many regulatory frameworks (PCI, HIPAA, FISMA, GLBA, NERC, SOX, GDPR, EU Data Directive, ISO, COBIT).

Splunk can ingest data from any source, which includes DLP, FIM, EDR, DAM and WAF tools, as well as from custom applications. Advanced security analytic capabilities are available from native machine-learning functionality and integration with Splunk UBA. Splunk's architecture consists of forwarders to bring data into the system, indexers that index and store raw machine

logs and search heads that provide access to the data via the web-based graphical user interface (GUI). Any component can be deployed on-premises, in the cloud or in combination.

Comparison with SHIELD:

Splunk is one of the most innovative and complete log management tools working as a SIEM tool for security management, monitoring, ticketing etc. Similar to the SHIELD DARE, it exploits a wide range of data sources and also uses machine learning to infer anomalies. It could be augmented with SHIELD's NFV capabilities in order to constitute a complete security infrastructure as-a-Service.

2.1.3.15. VSS of Nuage Networks (Nokia)

Description:

Nuage Networks[18] (from Nokia) provides Virtualized Security Services through its VSP (Virtualized Services Platform) solution. One of the services is the Virtualized Security Services (VSS) that it is a multitenant software-defined security solution for data centers and wide area network (WAN) environments.

VSS is a distributed, end-to-end (cloud, datacenter, and branch) software-defined network security, visibility, and automation solution. This solution provides security capabilities that provide contextual traffic visibility and security monitoring, as well as dynamic security automation for rapid incident response.

VSS supports a three-pronged security methodology with separate components and features to address each step in the security lifecycle:

1. VSS Prevent. Prevent security incidents by minimizing the attack surface with software-defined microsegmentation and policy enforcement across the cloud, datacenter, and WAN.

2. VSS Detect. Detect security threats and monitor compliance with contextual network visibility and security analytics in real-time.

3. VSS Respond. Respond faster to security incidents and breaches by automating remediation processes, such as quarantining suspicious applications or engaging deeper analysis tools.

Each component is based in proprietary products:

- VSS Prevent is a Layer 4 Firewall and forwarding routing rules for network segmentation.
- VSS Detect. Visualize traffic flows between groups of end points (policy groups) within a domain. Provides contextual visibility to east-west traffic between VMs, containers and bare-metal workloads inside the datacenter, as well as traffic crossing the branch perimeter to validate compliance with policy, monitor and alert on ACL policy violations for compliance and early threat detection, enables detection of security attacks based on abnormal spike in network traffic (e.g., during DDoS attack) and enables detection of advanced security attacks by selectively mirroring traffic to security analyzer for traffic that requires full packet inspection.
- VSS Respond. Automates responses while the attack is happening by taking dynamic policy action (e.g., insertion of advanced security services/mirroring of traffic).

[18] http://www.nuagenetworks.net/products/virtualized-security-services/

The VSP platform provide the Network Service Gateway (NSG), the router in the branch office, able to implement the security capacities and provide a SD-WAN service to implement VPNs between the branches of the customer.

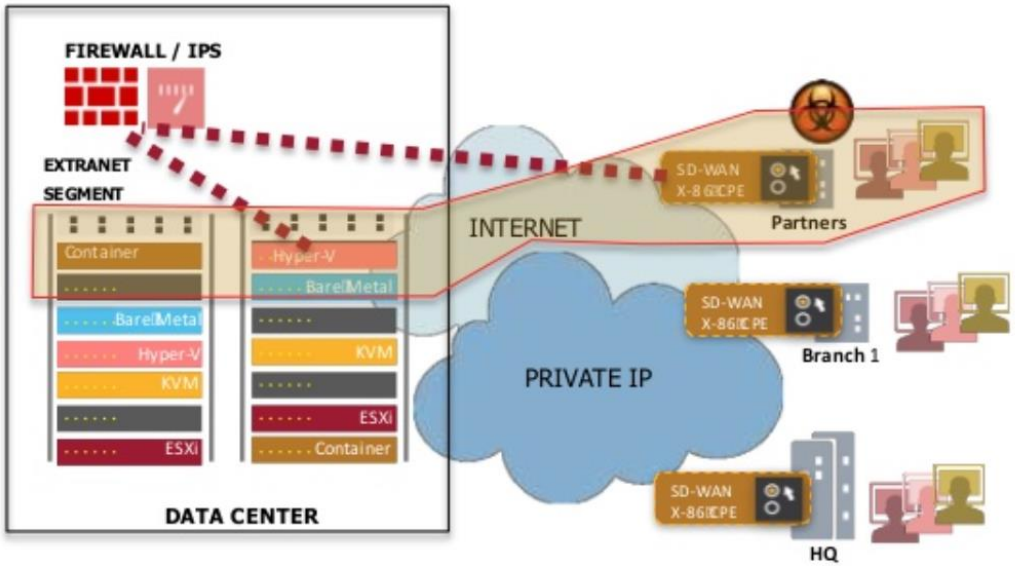


Figure 8. VSS architecture

This element, NSG, is also able to integrate VNFs of thirds parties.

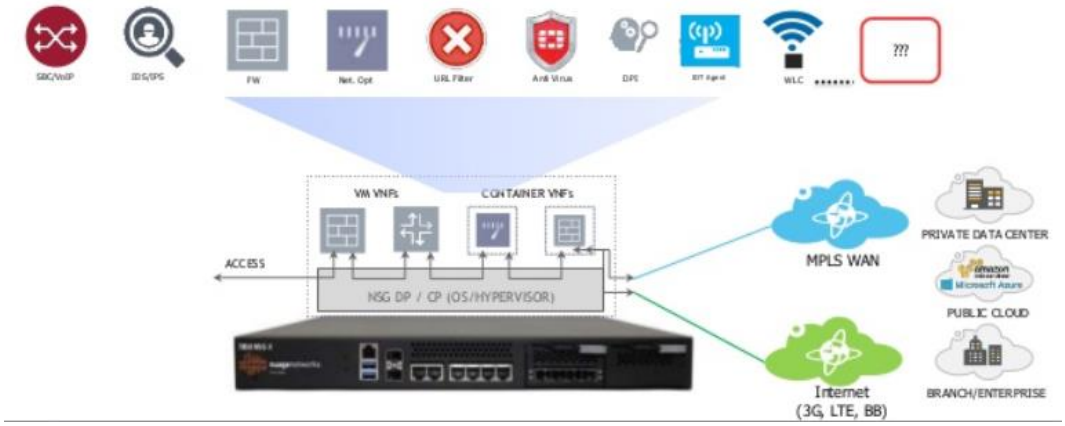


Figure 9. NSG third party integration

Comparison with SHIELD:

Nuage covers SHIELD's Use Case 1 protecting ISP data centers and the Use Case 2 providing security services to the Business clients. Nuage provide two solutions for the customer, the NSG in a baremetal solution or the virtualized NSG to install in a whitebox.

The overall Nuage solution seems very similar to the SHIELD framework. For example, VSS Detect protection is somehow related to DARE concepts, the NSG device security

functionalities, but the details show clear differences. VSS Detect is focused in metric visibility, not in artificial intelligence and correlations as DARE components support. It is also not clear how the integration with 3rd parties VNFs is supported.

2.1.4. 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 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 2.1.3.

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

Criteria / Capabilities	Description	Category
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 - Traffic redirection - Instantiation of new security functions	NFV + SDN Capabilities
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
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					✓	✓	✓							✓			✓	✓	✓

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
Incident Response and Management/ Built-in 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	✓	✓	✓		✓	✓	✓							✓			✓	✓	✓

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
Open Source code and integration	✓		✓	✓										✓					
Standards ETSI compliance	✓															✓			✓
Open API and protocols	✓	✓	✓	✓				✓			✓				✓	✓			✓
Integration of third-party vNSFs	✓										✓					✓			✓
Data exfiltration detection	✓							✓	✓			✓	✓						
L4/L7 Firewall	✓							✓		✓		✓					✓		✓
DDoS protection	✓							✓		✓							✓		✓

The above table (Table 3) presents a comprehensive capabilities comparison between SHIELD and other similar products that were described in 2.1.3. 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.

The versatility of SHIELD is acknowledged 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. More specifically, the DARE platform encapsulates typical SIEM features like real-time monitoring and advanced threat detection, while adding the novelty of parallel advanced analysis, offered by its two cybersecurity engines. Moreover, by relying on Big Data infrastructure, SHIELD ensures scalability and efficient load management in large enterprise environments. As a SecaaS solution, it facilitates deployment by requiring no on-premises software, being ideal for smaller organisations that are restricted by hardware costs or other technical limitations. As a product that offers SDN/NFV functionalities, it is able to orchestrate a number of virtualized monitoring and actuating services in order to achieve automated incident detection and response. The open-source nature of the majority of SHIELD's components grants access to developers who want to build, modify or integrate third-party services or exploit the engine's APIs and protocols. Finally, SHIELD's Trust Monitor incorporates infrastructure and service attestation mechanisms, which seem to be missing from the rest of the competitive products. All the above elements are indicative of SHIELD's innovative development, as well as of its great market potential.

2.1.5. 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.

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 seemingly 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.

2.1.6. SWOT Analysis

Figure 10 below illustrated the initial SWOT analysis available at the early stage of the project.

Figure 10. SWOT Analysis (from SHIELD proposal)

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 2.1.3). The prediction on how the market will evolve (see section 2.1.1) 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 11), in this case oriented to Managed Security Services Providers (MSSP).

Initial insights of previous sections, suggest that MSS (Managed Security Service) will be a potential service model for SHIELD, but detailed business model opportunities are being studied in T2.3 and it will be presented in D2.3. Nonetheless, next Figure 11 shows a specific SWOT analysis focused in technological dimension for above mentioned MSS.

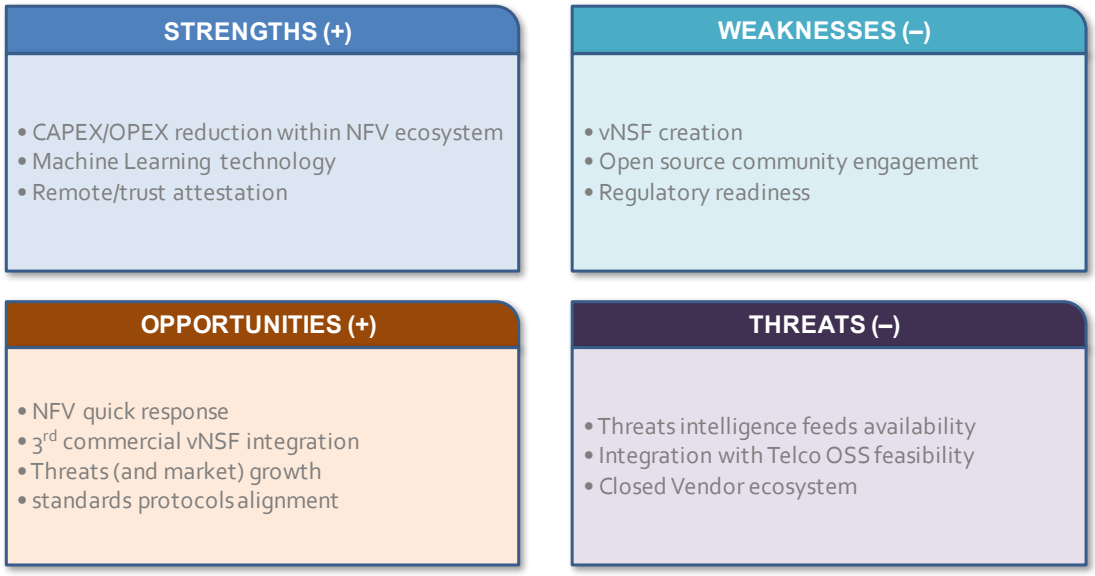


Figure 11. Technical SWOT Analysis for Managed Security Service (MSS)

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) show a clear path to relay upon Open Source MANO, and Apache Spot open source code. This is reinforced if the model enriches the respective open source communities.

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 movement is already being done by some commercial solutions (e.g. RAD and Nokia) by the strong market growth 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 messages. Lack of cyber threats feeds to increase the intelligence (directly in the DARE or using the vNSFs) should be faced.

Remote attestation today is a research domain, meanwhile commercial solutions are focused 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.

3. SHIELD ROADMAPPING

3.1. Roadmapping Criteria and Method

Following the market analysis which identified the main competitors of the SHIELD platform T6.3 proceeded by proposing a roadmap to maximize the chances of SHIELD commercialization in the different market segments. In order to complete this task, specific feedback is needed by collecting the expert's opinions from different stakeholders through standard techniques, such as questionnaires and focus groups.

The SHIELD consortium launched a survey, focusing on the factors that will affect market adoption and evolution of the SHIELD solution. Apart from the traditional method of collecting experts' opinions, the survey uses the Fuzzy Analytic Hierarchy Process (FAHP) methodology for the Criteria Comparison Part.

AHP [9][10] was already used for collecting the requirements listed in D2.1. AHP is a structured technique for dealing with complex decisions based on a rational and comprehensive framework for decomposing an unstructured complex problem into a multi-level hierarchy of interrelated criteria, sub-criteria and decision alternatives. By incorporating judgments on qualitative and quantitative criteria, AHP manages to quantify decision makers' preferences. The relative priorities of the criteria, sub-criteria and alternatives are finally calculated by a mathematical combination of all these various judgments. Each criterion (or sub-criterion) has been rated according to its degree of relative importance to another criterion (or sub-criterion) within the group in the basis of pair wise comparison. The consistency of replies has been tested.

However, AHP can be in some cases subjective and inaccurate, mainly due to its inability to adequately handle the inherent uncertainty and imprecision associated with the mapping of a decision-maker's perception to exact numbers. In this case, the Fuzzy Analytic Hierarchy Process (FAHP), an extension/improvement of the AHP methodology has been proposed [11]-[17] as a means to address this uncertainty. Fuzzy numbers are used in order to model the relative importance of criteria and sub-criteria (Methodology presented at Appendix A. Survey Questionnaire). Although Fuzzy AHP is proposed as a more accurate version of AHP, it is up to the researcher to decide between simple and Fuzzy AHP in order to balance between accuracy and complexity.

The use of fuzzy numbers as answers (vague comparisons), although increasing the processing complexity, provides for more accurate and meaningful results. A fuzzy weight for each criterion and subcriterion is evaluated, while crisp weights can also be obtained through the defuzzification process.

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

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

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

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

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

- Technology Enablers - Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed
    - Cloud/NFV/SDN Environment– Security Services running in the cloud outside or inside the company, supporting capacities for NFV+SDN management
    - Big Data technologies – Big Data technology applied (e.g. Hadoop, Spark etc.)
    - Open source - Open-source Solution, also implemented with open sourced tools and code, probably with commercial support behind
- SIEM (Security information and event management) like functionalities, functionalities like user behaviour analysis, advanced analytics and threat mitigation
    - Advanced threat mitigation - Automatic proposal of mitigation actions and enforcement of security through policies
    - Network & application analysis - Detection of ransomware activity, monitoring internet activity. Some examples are: access to files on file servers, identity root cause of bandwidth peaks on the network, abnormal application activity, application layer attack detection, fraud detection, including analytics such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization) to produce insights.
    - End User Monitoring/SUBA - Security User Behavior Analytics, risk based profiling and behavioral analytics to identify statistical anomalies for network, user and device activity.
- Platform Features – Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation
    - Support for third-party services and vNSFs – Capability of supporting third party services and different families of vNSFs, new vNSFs and analytics to adapt to new threats.
    - Data export and sharing - Data export and sharing with 3rd parties
    - Infrastructure and service attestation - Verification of the integrity of infrastructure and software, prevention of unauthorised modifications
- Performance - Performance aspects, such as real-time operation, high availability and multi-threat support

  - **Real Time Monitoring** - real-time views and threat visualizations of ongoing threat activity, collection of event data in near real time in a way that enables immediate analysis
  - **SECaaS** – Security as a service, High Availability of the security solution. Running the whole solution as a service, that allows scalability, redundancy and high availability
  - **Multi-threat support -** simultaneous attacks detection & mitigation
- **Business/Strategy aspects** - Market related issues and compliance issues
  - **Capex -> Opex transformation and flexible pricing –** Transforming the capital cost to Operational, lowering the threshold for players to enter the market, Solution with decreased cost, including lower installation and maintenance, equipment and SW costs. Flexible pricing model, per service, per use case, per data traffic, pay-as-you-go.
  - **Support for new Business Models** – Facilitating new players to enter the market, and traditional roles to be changed.
  - **Compliance to technological Standards** - support of open APIs, and standards protocols to be integrated with company systems and tools. This also includes data export and sharing capacity in standard formats.
  - **Compliance to data privacy policies (GDPR[19] etc.)** - Compliance to regulations and standards. No need for separate solutions for compliance, e.g.: privacy, audit and report.
- **Ease of Use** - Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity
  - **Built-in templates and workflows -** content management, management, event handling, use cases workflow to support incident response, Out-of-the-box use cases covering a variety of use cases, such as user activity monitoring, network monitoring, data exfiltration and malware activity, automation and out-of-the-box content, operational use cases (like templates).
  - **Scalability/ Modularity -** expandability of the platform, just by adding hardware resources. Ability for modular/incremental deployment.
  - **Deployment and Support Simplicity –** Easy setup, operations and maintenance; support for non-expert users.

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

[19] General Data Protection Regulation

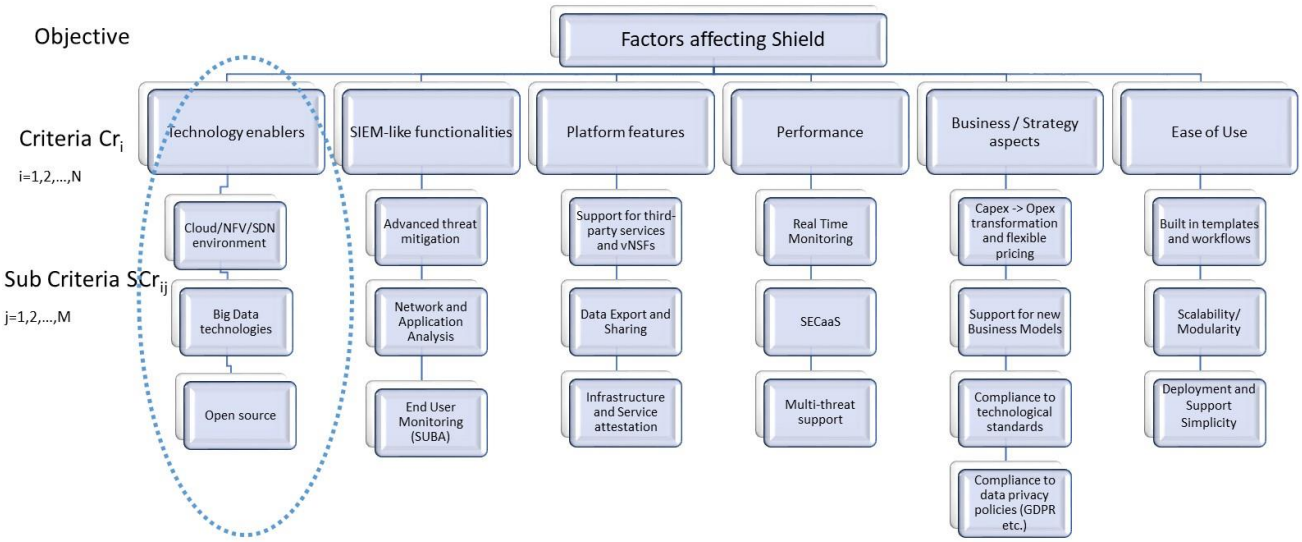


Figure 12. Multi-level hierarchy of interrelated criteria and sub-criteria.

This procedure is based on pairwise judgments of the experts from the second to the lowest level of the hierarchy. At each level, the criteria (and sub-criteria) are compared pair-wisely according to their degree of influence in the factors and based on the specified criteria at the higher level (dot lines grouping). The described comparisons are conducted using the standardized nine levels scale shown in Table 1 [9].

Table 1 - The Ranking Scale

Importance	Definition	Explanation
1	Equal importance	The two criteria contribute equally
3	Moderate importance	Experience and judgment favor one criteria
5	Strong importance	A criterion is strongly favored
7	Very strong importance	A criterion is very strong dominant
9	Extreme importance	A criterion is favored by at least an order of magnitude
2,4,6,8	Intermediate values	Used to compromise between two of the above numbers

The experts indicate their preference by providing a number that indicates the relative importance. In detail, experts were asked to determine the (sub-) criterion of his/her preference (for every pair of (sub-) criteria) and provide the upper and lower limit (range) of their relative importance using any number between 1 and 9. As shown in Table 1 when a criterion has an equal importance, it takes score (1). This usually happens when a criterion is compared to itself. When one criterion, compared to another, is of equal to moderate importance, it takes the score (2) and so on.

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

The online questionnaires were conducted and completed during a period of 1 month (middle October to middle November 2017) with the final set of 26 experts. From the 26 experts who initially participated in the survey, 5 questionnaires were discarded as inconsistent, since their associated Consistency Ratio (Both fake and random answers are characterised inconsistent by evaluating particular ratios and omitted from the calculations).

This sample (21 experts) can be assumed as a sufficient size for the purpose of a FAHP analysis since the changes in the probability rank reversal when an additional expert is added to the group are below 1% at M=15 (where M is the number of experts) [11]-[13].

The pairwise comparisons were conducted by a web-based survey/road mapping platform incorporating all elements of the FAHP framework, where experts accessed the platform and filled in the questionnaires. The web-platform was implemented using Lime Survey [14], an open source tool for web surveys, hosted by inCITES.

The responses were strictly anonymous, no personal data was collected during the survey, and a brief info-sheet was presented to the responder, to inform him/her of the scope and purpose of the survey.

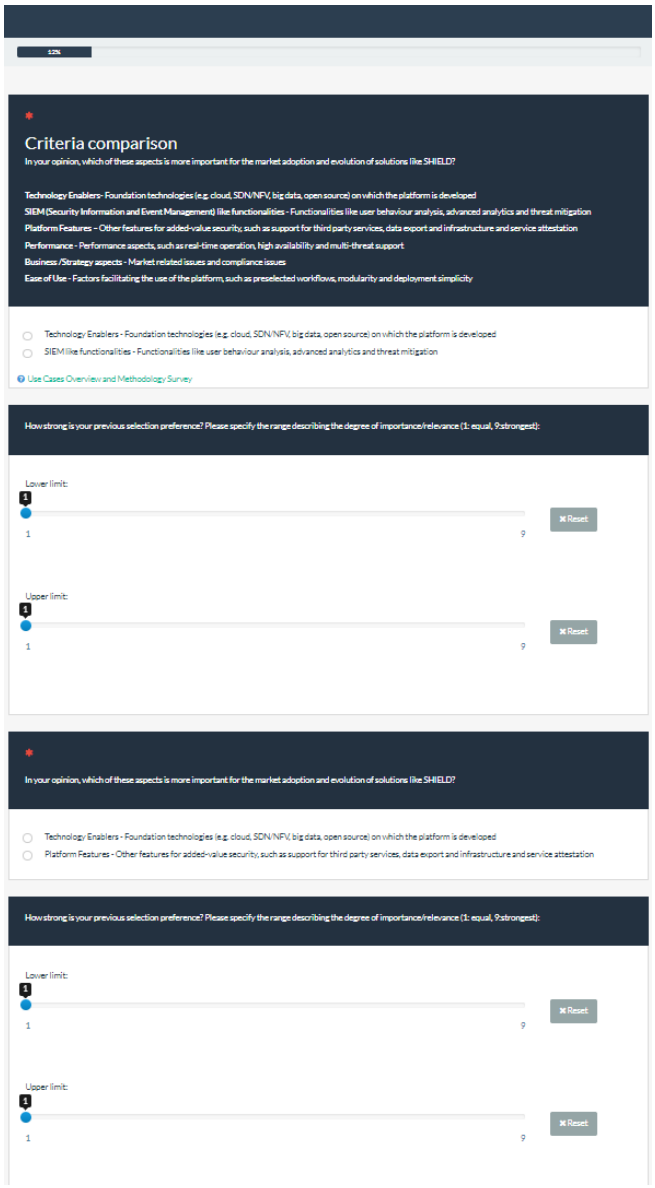


Figure 13 . SHIELD online Survey Tool - Snapshot

Since Lime Survey has not built-in modules to carry out a FAHP, the necessary calculations were performed using MATLAB [19], leading to an estimation of the weights signifying the importance of criteria and sub-criteria. In the begging of the survey, questions concerning the type of organization (Research centre, Academia, ISP/Operator, SME, Industry, Government Agency), the position in organization (Technical, Business) of the participants, as well as the size of their organization were posed. In Figure 14 the statistics of the participants' profiles are illustrated.

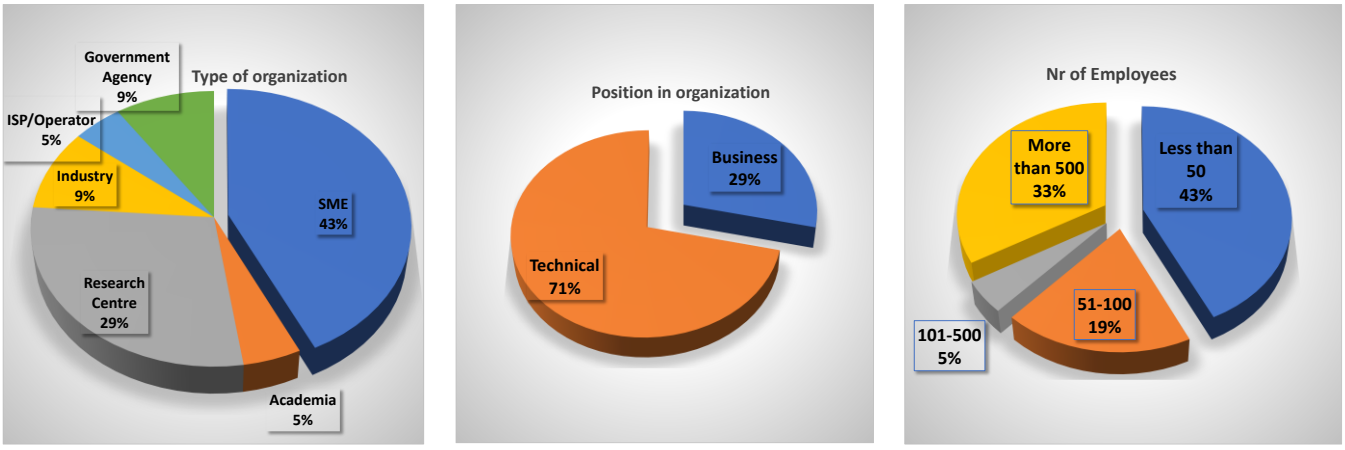


Figure 14. Statistics of the Participants

3.2. Evaluation Results and Discussion

3.2.1. Weighting of each criterion

In this section, we present and discuss the results of the survey regarding the factors that will influence market adoption and evolution of SHIELD solution. Using the methodology described above, both fuzzy and crisp weights can be estimated prioritizing the criteria and sub-criteria. The derived concerning the weights of the criteria (grey highlight) and the sub-criteria that are expected to affect market adoption and evolution SHIELD are shown in Table 4 and illustrated in Figure 15.

Table 4. Fuzzy and crisp weights of criteria and sub-criteria

(Ci)/ (SCij)	Criteria/sub-criteria	Description	Fuzzy weight	Crisp weight
C_1	**Technology Enablers**	Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed	(0.101; 0.134; 0.176)	0.1332
SC_{11}	**Cloud/NFV/SDN Environment**	Security Services running in the cloud outside or inside the company, supporting capacities for NFV+SDN management	(0.384; 0.486; 0.616)	0.4863
SC_{12}	**Big Data technologies**	Big Data technology applied (e.g. Hadoop, Spark etc.)	(0.226; 0.289; 0.369)	0.2892
SC_{13}	**Open source**	Open-source Solution, also implemented with open sourced tools and code, probably with commercial support behind	(0.178; 0.224; 0.285)	0.2245
C_2	**SIEM like functionalities**	Functionalities like user behaviour analysis, advanced analytics and threat mitigation	(0.107; 0.143; 0.191)	0.1429
SC_{21}	**Advanced threat mitigation**	Automatic proposal of mitigation actions and enforcement of security through policies	(0.372; 0.494; 0.652)	0.4938
SC_{22}	**Network & application analysis**	Detection of ransomware activity, monitoring internet activity. Some examples are: access to files on file servers, identity root cause of bandwidth peaks on the network, abnormal application activity, application layer attack detection, fraud detection, including analytics such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization) to produce insights.	(0.269; 0.35; 0.46)	0.3508

(Ci)/ (SCij)	Criteria/sub-criteria	Description	Fuzzy weight	Crisp weight
SC_{23}	**End User Monitoring/SUBA**	Security User Behavior Analytics, risk based profiling and behavioral analytics to identify statistical anomalies for network, user and device activity	(0.119; 0.156; 0.204)	0.1554
C_3	**Platform Features**	Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation	(0.121; 0.157; 0.208)	0.1576
SC_{31}	**Support for third party services and vNSFs**	Capability of supporting third party services and different families of vNSFs, new vNSFs and analytics to adapt to new threats.	(0.228; 0.304; 0.406)	0.3040
SC_{32}	**Data export and sharing**	Data export and sharing with 3rd parties	(0.092; 0.12; 0.159)	0.1204
SC_{33}	**Infrastructure and service attestation**	Verification of the integrity of infrastructure and software, prevention of unauthorised modifications	(0.424; 0.576; 0.778)	0.5756
C_4	**Performance**	Performance aspects, such as real-time operation, high availability and multi-threat support	(0.161; 0.214; 0.285)	0.2141
SC_{41}	**Real Time Monitoring**	Real-time views and threat visualizations of ongoing threat activity, collection of event data in near real time in a way that enables immediate analysis	(0.256; 0.343; 0.454)	0.3418
SC_{42}	**SECaaS**	Security as a service, High Availability of the security solution. Running the whole solution as a service, that allows scalability, redundancy and high availability	(0.293; 0.393; 0.529)	0.3944
SC_{43}	**Multi-threat support**	Simultaneous attacks detection & mitigation	(0.206; 0.264; 0.343)	0.2638
C_5	**Business/Strategy aspects**	Market related issues and compliance issues	(0.111; 0.149; 0.198)	0.1483
SC_{51}	**Capex -> Opex transformation and flexible pricing**	Transforming the capital cost to Operational, lowering the threshold for players to enter the market, Solution with decreased cost, including lower installation and maintenance, equipment and SW costs. Flexible pricing model, per service, per use case, per data traffic, pay-as-you-go.	(0.157; 0.206; 0.269)	0.2059
SC_{52}	**Support for new Business Models**	Facilitating new players to enter the market, and traditional roles to be changed.	(0.109; 0.144; 0.188)	0.1436
SC_{53}	**Compliance to technological Standards**	support of open APIs, and standards protocols to be integrated with company systems and tools. This also includes data export and sharing capacity in standard formats.	(0.172; 0.225; 0.294)	0.2248
SC_{54}	**Compliance to data privacy policies (GDPR etc.)**	Compliance to regulations and standards. No need for separate solutions for compliance, e.g.: privacy, audit and report.	(0.33; 0.426; 0.551)	0.4257
C_6	**Ease of Use**	Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity	(0.149; 0.203; 0.277)	0.2039
SC_{61}	**Built-in templates and workflows**	Content management, management, event handling, use cases workflow to support incident response, Out-of-the-box use cases covering a variety of use cases, such as user activity monitoring, network monitoring, data exfiltration and malware activity, automation and out-of-the-box content, operational use cases (like templates).	(0.146; 0.19; 0.245)	0.1897
SC_{62}	**Scalability/ Modularity**	Expandability of the platform, just by adding hardware resources. Ability for modular/incremental deployment.	(0.265; 0.346; 0.45)	0.3459

(Ci)/ (SCij)	Criteria/sub-criteria	Description	Fuzzy weight	Crisp weight
SC_{63}	**Deployment and Support Simplicity**	Easy setup, operations and maintenance; support for non-expert users.	(0.363; 0.464; 0.596)	0.4644

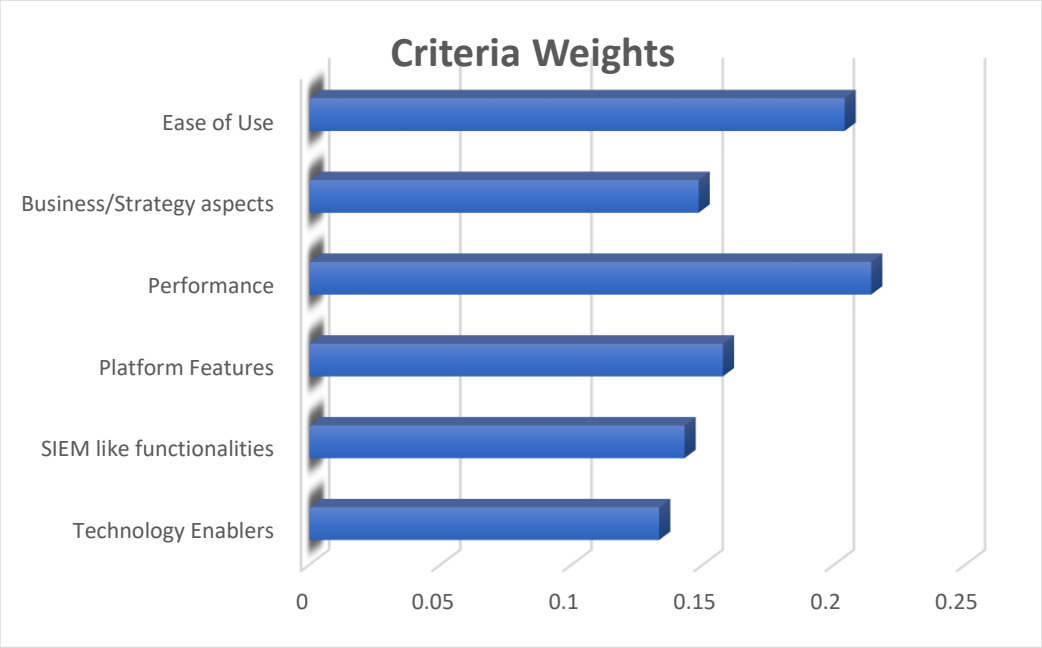


Figure 15. Relative weights of SHIELD market adoption and evolution criteria.

It is notable, that according to the opinion of the experts, the criterion that is the most important one to take into account as its weight reaches 0.215 is that of Performance. This is also a confirmation of the experts that are now waiting for new technological innovations in order to support the advanced services and applications in terms of increased performance with their increased requirements in Real time monitoring, SECaaS and Multi-threat support. Taking into account the high priority of performance, it can be deduced that the performance KPIs therefore need to be reached independently of the underlying technology. Performance is followed by the Ease to Use criterion giving the implication that future solutions should be as responsive as possible and at the same time it should not be complicated for the detection of the threats. The remaining criteria are of equal importance indicating that the vendors/providers should give the same attention in the development of their solution, since their ranking can change in the near future.

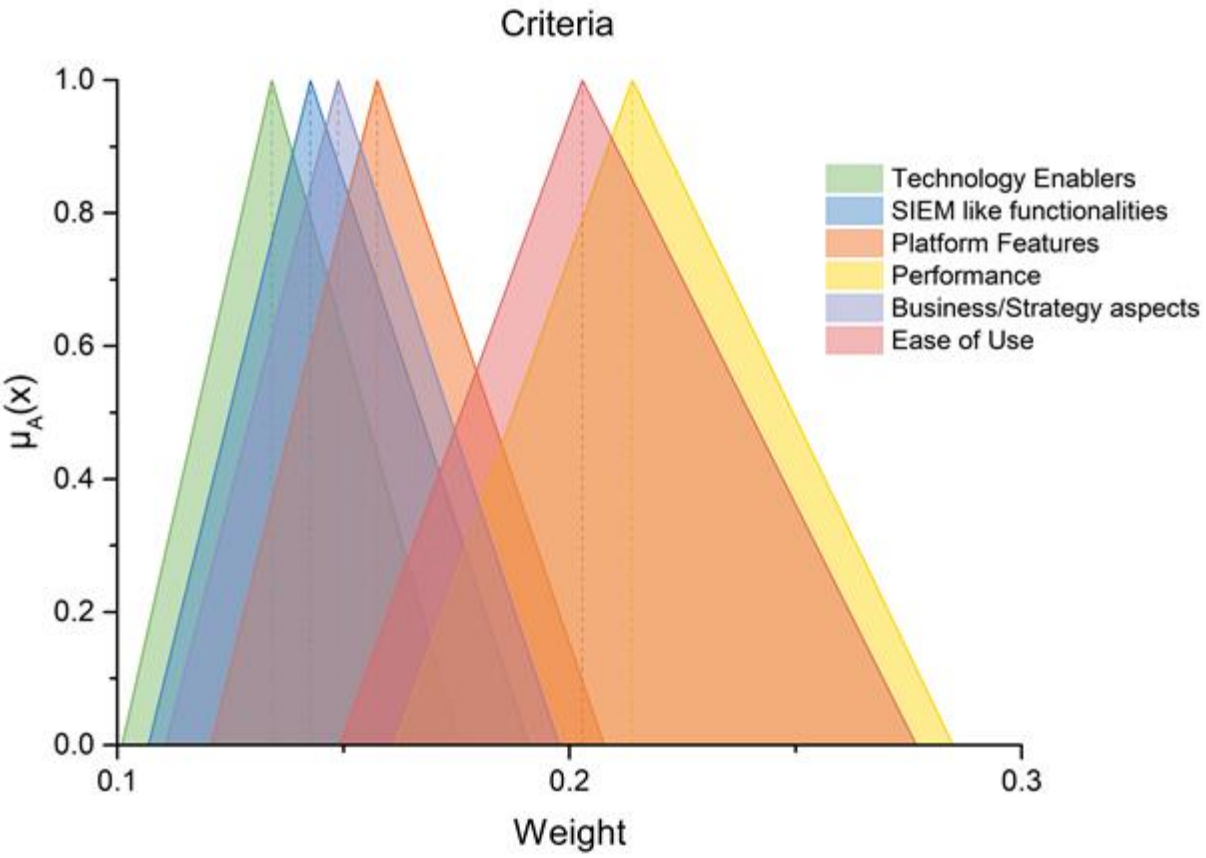


Figure 16. Fuzzy evaluation of Criteria.

It is also interesting to investigate the ranking of criteria using the fuzzy weights (Figure 16). If we had to make a definite choice between the relevant criteria, Performance should be chosen in conjunction with Ease to use. However, decision making does not always imply a choice between alternatives; but also references the probabilities, possibilities or considerations concerning opportunities vs. risks. The fuzzy numbers can then be taken to guarantee the minimum and maximum values. An a-cuts can also be taken into account in order to define narrower lower and upper limits of the relevant weightings based on risk considerations. Figure 16 illustrates that there is a large degree of overlapping between the two first (Performance and Ease of Use) the four last criteria (Business/Strategy aspects, SIEM like functionalities, Platform Features, Technology Enablers). This is a clear indication that the ranking of these criteria may possibly change (a situation referred to as rank reversal) for the two first and for the rest one, especially when the solutions will become more mature.

Also note that the Performance and Ease to Use criterion are more prone to uncertainty-induced perturbations since their shape (i.e., width) which are wider than the remaining four criteria; the rest four criteria have narrowest width, additionally indicating confidence among the experts that they really are the least important considerations in the deployment for similar solutions like SHIELD but the order can change because of the overlapping. The experts suggest that the ranking of these criteria can possibly change and even the Technology enablers could be higher in the factors affecting the evolution of similar solutions like SHIELD especially when the experts will become more familiar with the achievements of new technologies.

3.2.2. Weighting of Sub-criteria under each criterion

The second step for the evolution of the critical factors is the examination of the weights of the sub-criteria under each criterion.

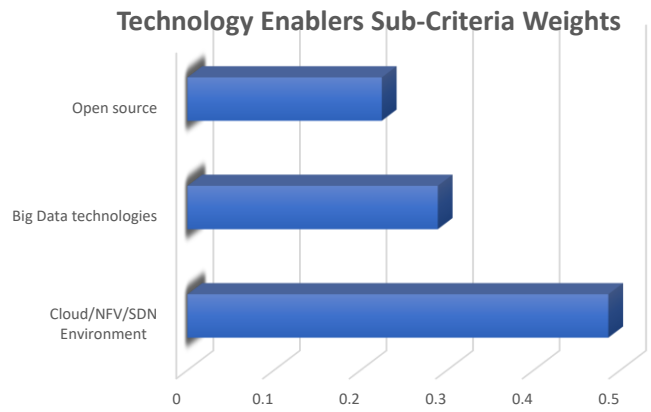


Figure 17. Relative weights of Technology Enablers C1 Sub-criteria.

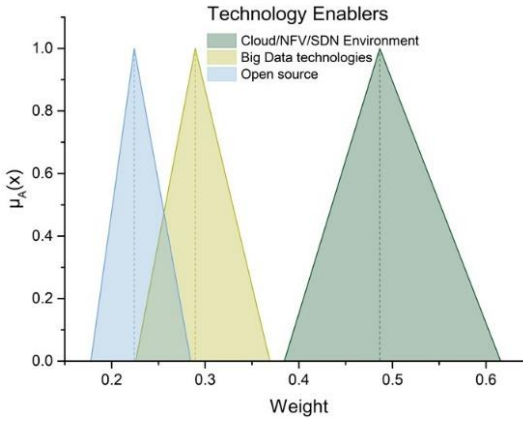


Figure 18. Fuzzy evaluation of Technology Enablers C_1 Sub-criteria.

As shown, the most important factor (almost 0.5 weight) for Technology Enablers of SHIELD is Cloud/NFV/SDN environment with no overlapping with the remaining criteria. Security Services running in the cloud outside or inside the company, virtualization technologies using SDN and NFV are anticipated to drastically affect the development of cybersecurity solutions. This is also confirmed by the trend of the telecom industry that is moving quickly to virtualized and software-controlled solutions, as well as by a number of market reports forecasting rapid growth of these technologies. Open source implementation, probably based on commercial support, are of less importance for the experts as stated in the vast majority of the competitors in the previous chapter. Fuzzy numbers evaluation for Big Data and Open source illustrate that the ranking between them could change.

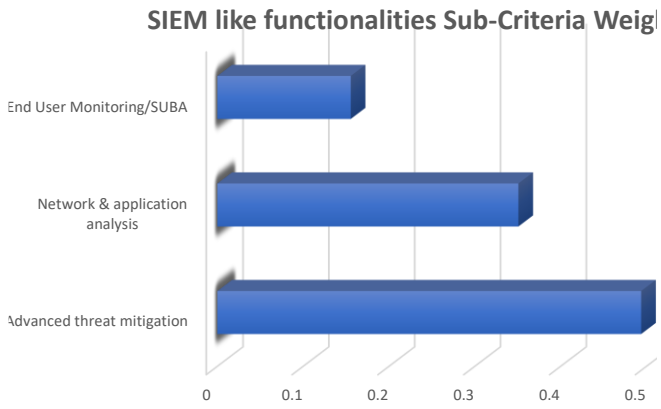


Figure 19. Relative weights of SIEM like functionalities C_2 Sub-criteria.

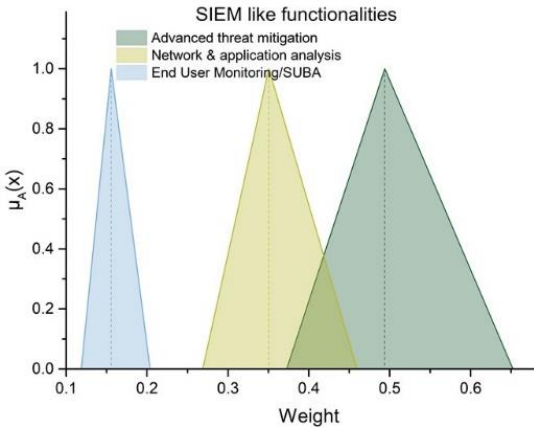


Figure 20. Fuzzy evaluation of SIEM like functionalities C_2 Sub-criteria.

Advanced threat mitigation is of major importance (~0.5) for SIEM like functionalities. As expected, automatically proposed mitigation actions are preferable for the experts since the ability of taking decision could elaborate their effectiveness. The second sub criterion, Network & application analysis where detection of ransomware activity and monitoring internet activity takes place is of great importance in the traditional functionalities since most of the experts are familiar with similar implementation and there is a real need for analytics, machine learning in order to produce insights. The high degree of overlapping (fuzzy evaluation) indicates that the ranking between these two could change. End User Monitoring/SUBA profiling and behavioral analytics to identify statistical anomalies for network and user are considered of less importance.

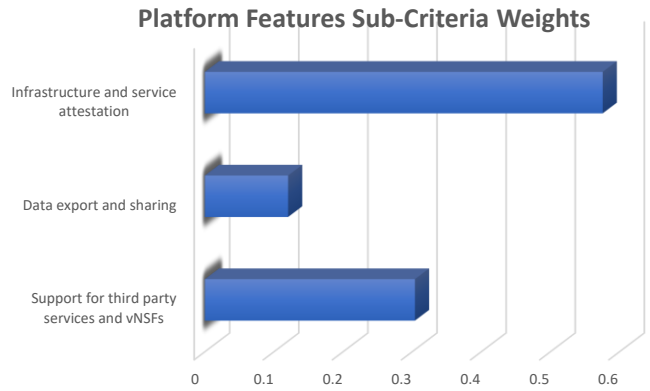


Figure 21. Relative weights of Platform Features C_3 Sub-criteria.

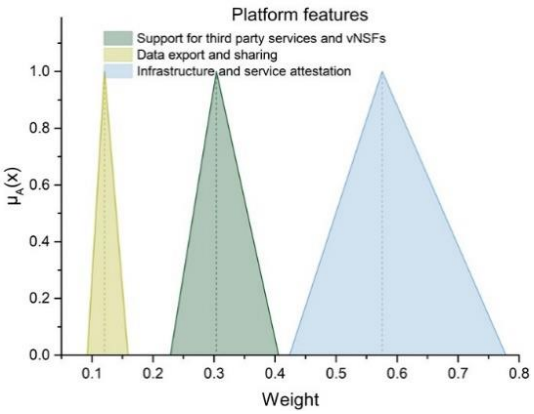


Figure 22. Fuzzy evaluation of Platform Features C_3 Sub-criteria.

In the pairwise comparison, experts believe that SHIELD evolution concerning Platform features is more relevant to Infrastructure and service attestation (more than 0.5) with no overlapping in the fuzzy evaluation. It can be seen that the ranking between the two first platform features cannot change due to no overlapping between them. So this is a clear result that incorporating infrastructure and service attestation mechanisms is of major importance. This capability seems to be missing from the rest of the competitive products in the previous chapter, which can eventually prove to be an important competitive advantage for SHIELD. Service attestation is followed by Support for third party services and vNSFs (1/3 of the pairwise comparisons) meaning that incorporating new actuating services in order to achieve automated incident detection and response is of great importance for the experts. Data export and sharing are of less importance for the market adoption, even if export in standard formats or proprietary with IoC could be mandatory for such systems. They might be part of the new proposed system but not the driver.

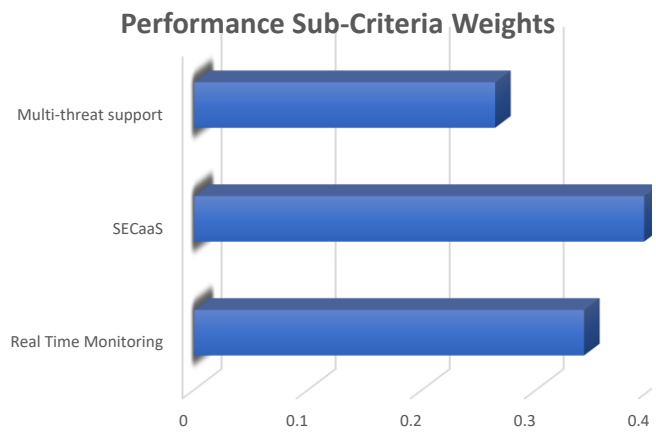


Figure 23. Relative weights of Performance C_4 Sub-criteria.

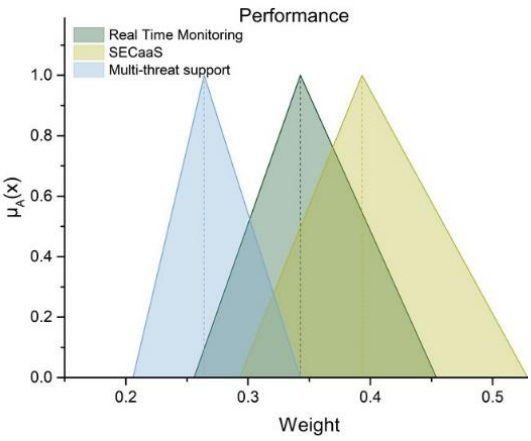


Figure 24. Fuzzy evaluation of Performance C_4 Sub-criteria.

In the Performance category, SecaaS is considered of major importance followed by Real Time Monitoring. This precipitates the selection of SHIELD for an ISP in order to provide advanced SecaaS services to its customers as the endorsed solution and at the same time this is a clear indication that SHIELD solution could start in the market as a service even if the ranking could change due to overlapping in the two criteria. This is expected since SecaaS ensures high availability by running the whole solution as a service allowing in parallel scalability and redundancy. Simultaneous attacks detection & mitigation with Multi threat support are in the third position with almost equal weight. This order is prone to uncertainty-induced perturbations because of its width and it could be easily rearranged since the experts are not confident about the pairwise comparison between real time monitoring and multi threat support.

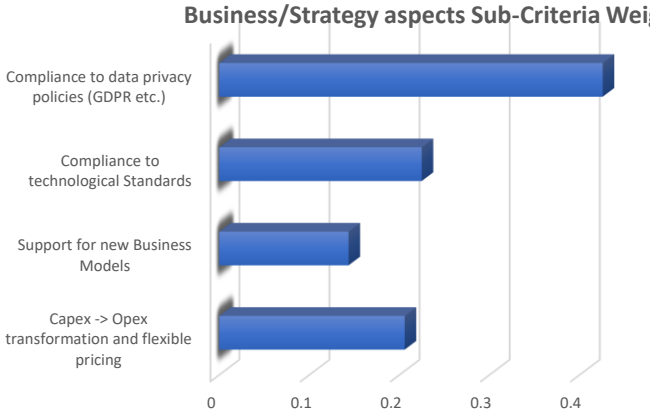


Figure 25. Relative weights of Business/Strategy aspects C_5 Sub-criteria.

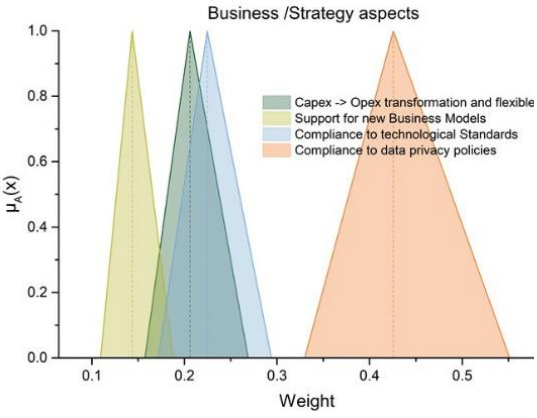


Figure 26. Fuzzy evaluation of Business/Strategy aspects C_5 Sub-criteria.

In the Business/Strategy domain, it is interesting enough that Compliance to data privacy and compliance to technological standards are ranked in the two first positions with the Compliance to data privacy policies like GDPR being the preponderant of the sub-criteria. This is mainly due to the fact that compliance acts inside the ISP logic where provider's issues like confidence/privacy/standards are of great importance. Furthermore the GDPR enforcement

regulation, approved in 2016, affects the whole market, and experts are well aware about this issue. In addition, according to the experts' opinions, cost reduction via transformation Capex to Opex is in the third place (weight: 0.20 close to the second: 0.22). This is not surprising as the cost of deployment is very important since it will influence services prices leading to increased or decreased penetration. CAPEX transforming to OPEX is one of the main characteristics stemming from the use of NFV; that is the softwarization of networks. Several networking functions, which traditionally required specialized network components are now being implemented as software modules in virtual machines. This is accompanied by a significant reduction in CAPEX, a portion of which is transformed to OPEX needed for the development and maintenance of such modules. Last but not least, the experts' opinion is that the new business models could not heavily affect this market adoption compared to compliance and capex reduction. Thus, as a choice firstly the solution should be compliant to regulations and the innovation in the business domain could follow.

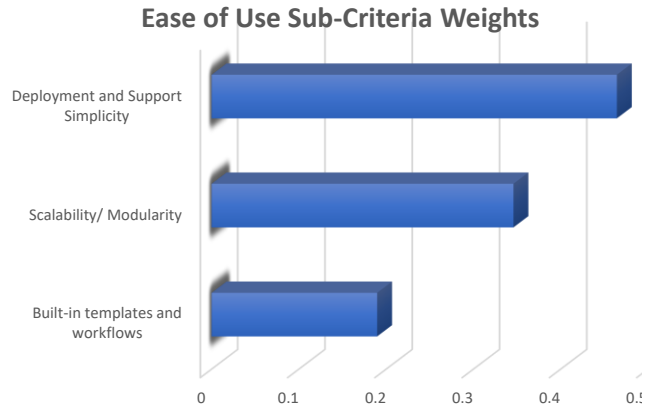


Figure 27. Relative weights of Ease of Use C_6 Sub-criteria.

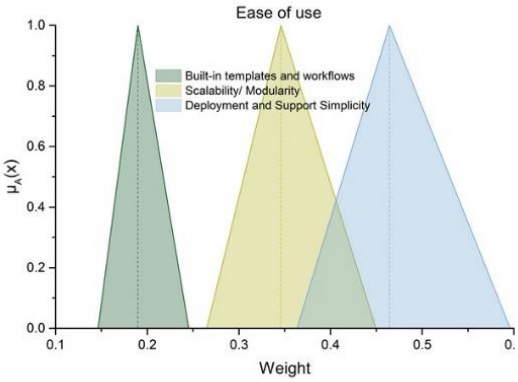


Figure 28. Fuzzy evaluation of Ease of Use C_6 Sub-criteria.

Regarding the sub-criteria of the Ease of Use criterion, it is clear that Deployment and Support Simplicity as well as Scalability/Modularity are the most important ones. This is usually stemming from the need for more rapid scalability and modularity in order to address the expandability of the platform (high demand), as well as for a more efficient network resource provisioning with modular/incremental simple deployment. Fuzzy analysis suggests that there is an overlapping indicating that the ranking of these sub-criteria may possibly change. The built-in templates and workflows are considered of lesser importance, probably due to the fact that such activities are anyway performed by experienced personnel. The message derived from such evaluation (Ease of use criteria) concerning the SHIELD cybersecurity solution, is to be as simple as possible in its deployment and installation, with scalability ability in order to be adapted in a new or legacy system.

3.2.3. Global priorities of sub-criteria

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

Table 5. Global Priorities of sub-criteria

(SCij)	Sub-criteria	Global Priority
SC_{63}	**Deployment and Support Simplicity**	9.50%
SC_{33}	**Infrastructure and service attestation**	9.10%
SC_{42}	**SECaaS**	8.40%
SC_{41}	**Real Time Monitoring**	7.30%
SC_{21}	**Advanced threat mitigation**	7.10%
SC_{62}	**Scalability/ Modularity**	7.10%
SC_{11}	**Cloud/NFV/SDN Environment**	6.50%
SC_{54}	**Compliance to data privacy policies (GDPR etc.)**	6.30%
SC_{43}	**Multi-threat support**	5.60%
SC_{22}	**Network & application analysis**	5.00%
SC_{31}	**Support for third party services and vNSFs**	4.80%
SC_{12}	**Big Data technologies**	3.90%
SC_{61}	**Built-in templates and workflows**	3.90%
SC_{53}	**Compliance to technological Standards**	3.30%
SC_{51}	**Capex -> Opex transformation and flexible pricing**	3.10%
SC_{13}	**Open source**	3.00%
SC_{23}	**End User Monitoring/SUBA**	2.20%
SC_{52}	**Support for new Business Models**	2.10%
SC_{32}	**Data export and sharing**	1.90%

The results presented in both the previous section and Table 5 are a valuable tool for decision and policy makers. In fact, they provide very useful guidelines for the successful evolution of cybersecurity solutions as well as for the fast market adoption of SHIELD like solutions.

As shown, the most important factors expected to affect the adoption of similar deployments in general are Deployment and Support Simplicity, Infrastructure and service attestation, and SECaaS. Essential the issues (sub-criteria) that are expected to significantly affect the market adoption and evolution of SHIELD solution are included in the three criteria/factors namely: Performance, Ease of Use and Platform Features. It is then evident the proposed solution should be elaborated with high availability, deployments simplicity and with advanced features. On the contrary less important are: End User Monitoring/SUBA, Support for new Business Models and Data export and sharing, indicating that even traditional business models are more trustable for the clients and on the other hand SUBA and data export could be characterized as unimportant or trivial solutions. The experts probably specify that the new business models could not heavily affect this market which is largely dominated by significant players.

4. INDIVIDUAL EXPLOITATION PLANS

This chapter presents the individual exploitation plans of each partner, as updated since the proposal preparation, taking into account the lessons learnt from Y1 developments. The final versions of the exploitation plans will be presented in the second edition of this deliverable (D6.4).

4.1. 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 wants 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 focuses 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 example is the upstreaming of a Linux patch to enhance the TPM performances for all Linux-based platforms [20].
2. Demonstration of the Trust Monitor in order to drive the industry towards secure monitoring of infrastructures using Trusted Computing technologies.

4.2. I2CAT

I2CAT is a key player in the European research environment around novel network management models, such as SDN and NFV. Moreover, I2CAT has recently signed an agreement with the Catalan Government and CESICAT (The Catalan cybersecurity agency) to lead and coordinate all the research done in cybersecurity in the region of Catalonia. As an organisation with a lot of experience in NFV orchestrators, I2CAT plans to exploit OSM (the SHIELD selected orchestrator) being one of the top most experts regarding this technology. In addition, given the strong focus on technology transfer of I2CAT, we plan to transfer into market this knowledge helping organizations to adopt OSM as their NFV orchestrator. Furthermore, considering the nature of I2CAT – i.e. a research centre aiming at bridging the gap between academic research and industrial innovation, the collaboration with key players in the global ICT market, and some key innovative SMEs focused in network management, machine learning, and NFV-enabled solutions, will strengthen the industrial impact of the research centre in both the regional and national area. As a leader of the cybersecurity roadmap in Catalonia, I2CAT aims to use SHIELD to leverage the potential of research and drive it into the innovation framework of NFV and SDN that permits much more flexible and fast-response research.

4.3. 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 their portofilo of consulting services and intensify its position as a reference international center of excellence for cybercrime from the business perspective.

4.4. 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.
- 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 [21].

4.5. 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 is already

involved in a number of 5GPPP Phase 1 and Phase 2 projects). 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.

4.6. 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[20] 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[21] 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. Orion positions itself in these growing markets, including (but not limited to) the following value propositions:

- 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.

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

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

4.7. 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 will be used in courses at master level, to enrich the syllabus with advanced security topics, and as subject for MSc and PhD dissertations. For research, the results will constitute the foundation for further proposals related to trust and security of SDN, NFV, and cloud infrastructures. Finally, for consultancy, the results will permit 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.

4.8. 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.

4.9. 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. Towards this end, Talaia will investigate the possible exploitation of any new algorithms and types of attacks that will be successfully tested and evaluated within the activities of SHIELD.

4.10. 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[22]. 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.

TID's exploitation plan will be comprised of several actions during and 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 is in active progress within Telefonica Data unit (LUCA) and Telefonica cybersecurity Unit (11Paths). The SHIELD frameworks model, and technical results, has been presented and discussed already. Furthermore, in the cybersecurity area a public webinar event[23] with Telefonica data unit (LUCA) has already been done. 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[24] service or Clean Pipes[25] product.

Also, the long-term plans focus in rollout a SHIELD business model integrated with network evolution services. Some potential areas in discussion are: SD-WAN[26] with some centralized vNSFs based security services, or universal CPE (uCPE)[27] with vNSFs deployed in a whitebox CPE.

4.11. 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

[22] https://www.telefonica.com/en/web/about_telefonica/in-brief
[23] 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
[24] https://www.elevenpaths.com/managed-security-operations
[25] https://www.elevenpaths.com/technology/clean-pipes
[26] https://www.sdxcentral.com/sd-wan/definitions/essentials-sd-wan-architecture/
[27] https://www.sdxcentral.com/articles/contributed/understanding-use-universal-cpe/2017/07/

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. By having a participation in this activity, Ubiwhere intends to maintain an open VNF ecosystem allowing SMEs to develop and provide their solutions to ISPs (using OSM) not being overwhelmed by the big industry vendors.

Network security analysis and mitigation component of SHIELD (DARE) is also of great interest to Ubiwhere. As a smart city developer and deployer, Ubiwhere is currently facing some potential network security problems that can be mitigated with the instantiation of a component with the same architecture and technologically ecosystem as DARE.

5. CONCLUSIONS

This Deliverable provides an initial report on SHIELD activities related to exploitation planning, including: analysis of global cybersecurity market and environment, identification of SHIELD positioning in the market and its unique value proposition. This deliverable also identifies the barriers that may limit system's development as well as the factors that influence the success of the proposed technological solution. All SHIELD partners contributed to this endeavour, achieving consensus among the consortium members for the factors affecting the evolutions of the proposed solution.

The cybersecurity market is estimated to grow substantially during the years to come and a large number of competitors are already dominating the market, offering products and services with comparable capabilities. From our analysis, it seems that there does not exist a commercial and integrated solution offering both SIEM features and advanced mitigation capabilities tailored for virtual network services. The versatility of SHIELD is acknowledged 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.

On the other hand, SHIELD is a newcomer on a very competitive market, populated mostly by companies that are pioneers 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.

A resource-demanding activity related to the exploitation planning was also the identification, evaluation and analysis of the factors that will affect market adoption and evolution of the SHIELD solution. According to the results derived from the survey, Performance seems to rank as the most important criterion that will affect SHIELD market adoption and evolution. It appears that breakthroughs in performance as are expected to be the main drivers behind cybersecurity solutions. The next most important criteria are these of Ease of use and Platform features, followed by Business/Strategy aspects, SIEM like functionalities and Technology Enablers. The last three criteria are of equal importance indicating that the vendors/providers should give the same attention in the development of their solution, since their ranking can change in the near future.

All the above mentioned conclusions, as well as the lessons learnt from the Y1 activities, helped the SHIELD partners to update their exploitation plan and better position their ambition with respect to the project results.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

[12] G. Dede, et al., "Convergence properties and practical estimation of the probability of rank reversal in pairwise comparisons for multi-criteria decision making problems," European Journal of Operational Research, vol. 241, pp. 458-468, 2015.

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

[14] D.-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," European Journal of Operational Research, vol. 95, pp. 649-655, 1996.

[15] P. J. M. van Laarhoven and W. Pedrycz, "A fuzzy extension of Saaty's priority theory," Fuzzy Sets and Systems, vol. 11, pp. 229-241, 1983/01/01 1983.

[16] T.-H. Chang and T.-C. Wang, "Using the fuzzy multi-criteria decision making approach for measuring the possibility of successful knowledge management," Information Sciences, vol. 179, pp. 355-370, 2009.

[17] I. Neokosmidis, et al., Assessment of socio-techno-economic factors affecting the market adoption and evolution of 5G networks: Evidence from the 5G-PPP CHARISMA project, In Telematics and Informatics, Volume 34, Issue 5, 2017, Pages 572-589, ISSN 0736-5853.

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

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

[20] 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.

[21] 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
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
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
MANO	Management & Orchestration
MSSP	Managed Security Service Providers
NF	Non-Functional (requirement)
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
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
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
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

APPENDIX A. SURVEY QUESTIONNAIRE

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

Survey for factors that will affect market adoption and evolution of SHIELD solution[28].

Welcome to SHIELD's survey regarding the factors that will influence market adoption and evolution of SHIELD solution. This survey is designed to gather information about factors influence the adoption of similar solutions related to the SHIELD project.

This survey does not involve the collection of personal data. All responses are anonymous and will not be linked to any individual.

SHIELD in a nutshell

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

Specifically, SHIELD studies 3 use-cases (small description of the use cases in a different web page):

[28] http://incites.eu/poll/index.php/586584

Methodology

Please answer the questions using the following instructions:

Each criterion will be rated according to its degree of relative importance to another criterion within the group in the basis of pair wise comparison. The consistency of replies will be tested. Please indicate your preference by providing a range [lower bound, upper bound] between 1 and 9 using the sliders.

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

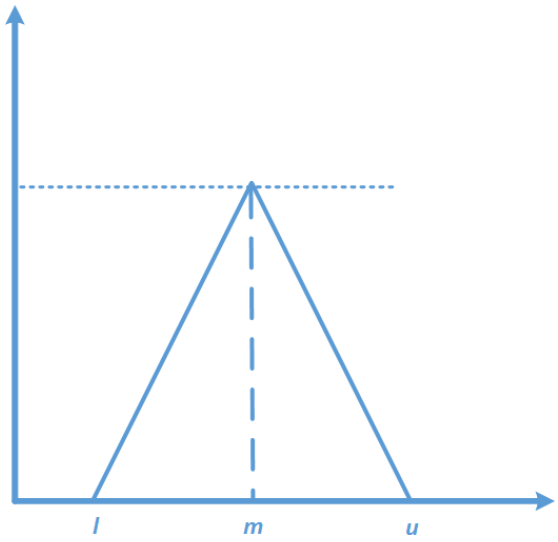
The scale used to find pair wise relative importance is a nine point scale as follows:

Importance	Definition	Explanation
1	Equal importance	The two criteria contribute equally
3	Moderate importance	Experience and judgment favor one criteria
5	Strong importance	A criterion is strongly favored
7	Very strong importance	A criterion is very strong dominant
9	Extreme importance	A criterion is favored by at least an order of magnitude
2,4,6,8	Intermediate values	Used to compromise between two of the above numbers

To deal with vagueness of human thought, the fuzzy set theory oriented to the rationality of uncertainty was introduced. A major contribution of fuzzy set theory is its capability of representing vague data.

A fuzzy set is a class of objects with a membership function ranging between zero and one. It was specifically designed to mathematically represent uncertainty and vagueness. Fuzzy set theory implements groupings of data with boundaries that are not sharply defined (i.e. fuzzy).

In this survey, triangular fuzzy numbers (TFN) are used in order to provide answers. This is the special class of fuzzy number whose membership is defined by three real numbers, expressed as **(l, m, u)** where l and u is the lower and the upper limit respectively and m is their middle. This is illustrated at the next figure:



l and u define the limits of the answers: if you are uncertain about your choice the range must be higher. The smaller the range between u and l the biggest the certainty regarding your answer.

Examples:

If the criteria are C1 and C2 and you select C1:
• An answer of 8.7 – 9 shows that C1 has extreme importance and you have high confidence at this choice
• An answer of 4.3 - 8.9 shows that C1 has a strong importance but you are not so certain about your choice
• An answer of 1 – 1.2 shows that C1 is almost equal to C2 with high confidence

Questions

By completing this survey, you allow the SHIELD partners to use this information to extract the importance of several factors involved in the SHIELD platform.

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

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

Profiling

1. Type of organization (dropdown menu)

- *Research centre*
- *Academia*
- *ISP/Operator*
- *SME*
- *Industry*

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

- *Technical*
- *Business*
- *Other*

3. Rank your familiarity with cyber security solutions

(low, medium, high)

4. How many employees work in your company?

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

Criteria

1. In your opinion, which of these aspects is more important for the market adoption and evolution of solutions like SHIELD?

   How strong is your previous selection preference? Please specify the range describing the degree of importance/relevance (1: equal, 9: strongest)

   Lower limit (number indication with a bar)
   Upper limit (number indication)

Technology Enablers - Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed

SIEM (Security information and event management) like functionalities, functionalities like user behaviour analysis, advanced analytics and threat mitigation

Platform Features – Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation

Performance - Performance aspects, such as real-time operation, high availability and multi-threat support

Business/Strategy aspects - Market related issues and compliance issues

Ease of Use - Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity

Technology Enablers	1	2	3	4	5	6	7	8	9	SIEM like functionalities
Technology Enablers	1	2	3	4	5	6	7	8	9	Platform Features
Technology Enablers	1	2	3	4	5	6	7	8	9	Performance
Technology Enablers	1	2	3	4	5	6	7	8	9	Business /Strategy aspects
Technology Enablers	1	2	3	4	5	6	7	8	9	Ease of Use
SIEM like functionalities	1	2	3	4	5	6	7	8	9	Platform Features
SIEM like functionalities	1	2	3	4	5	6	7	8	9	Performance
SIEM like functionalities	1	2	3	4	5	6	7	8	9	Business /Strategy aspects
SIEM like functionalities	1	2	3	4	5	6	7	8	9	Ease of Use
Platform Features	1	2	3	4	5	6	7	8	9	Performance
Platform Features	1	2	3	4	5	6	7	8	9	Business /Strategy aspects
Platform Features	1	2	3	4	5	6	7	8	9	Ease of Use
Performance	1	2	3	4	5	6	7	8	9	Business /Strategy aspects
Performance	1	2	3	4	5	6	7	8	9	Ease of Use
Business /Strategy aspects	1	2	3	4	5	6	7	8	9	Ease of Use

Importance of the Technology Enablers

This section compares sub-criteria related to Shield Technology Enablers factors.

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding Technology Enablers?

2. Please specify the range describing the degree of importance/relevance (1: equal, 9: strongest).

Cloud/NFV/SDN Environment– Security Services running in the cloud outside or inside the company, supporting capacities for NFV+SDN management (Decouple software and hardware using general purpose devices, and data from control planes)

Big Data technologies – Big Data technology applied (e.g. Hadoop, Spark etc.)

Open source - Open-source Solution, also implemented with open sourced tools and code, probably with commercial support behind

Cloud/NFV/SDN Environment	1	2	3	4	5	6	7	8	9	Big Data technologies
Cloud/NFV/SDN Environment	1	2	3	4	5	6	7	8	9	Open source
Big Data technologies	1	2	3	4	5	6	7	8	9	Open source

Importance of the SIEM-like functionalities

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding SIEM-like Functionalities?

3. Please rate the importance (pairwise comparison) of each one of the SIEM-like Functionalities of a cybersecurity solution

Advanced threat mitigation - Automatically propose mitigation actions and enforce security through policies

Network & application analysis - Detection of ransomware activity, monitoring internet activity. Some examples are: access to files on file servers, identity root cause of bandwidth peaks on the network, abnormal application activity, application layer attack detection, fraud detection, including analytics such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization) to produce insights.

End User Monitoring/SUBA - Security User Behavior Analytics, risk based profiling and behavioral analytics to identify statistical anomalies for network, user and device activity

Advanced threat mitigation	1	2	3	4	5	6	7	8	9	Network & application analysis
Advanced threat mitigation	1	2	3	4	5	6	7	8	9	End User Monitoring/SUBA
Network & application analysis	1	2	3	4	5	6	7	8	9	End User Monitoring/SUBA

Importance of the Platform Features

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding Platform Features?

4. Please rate the importance (pairwise comparison) of each one of the Platform Features of a cybersecurity solution

Support for third-party services and vNSFs – Capability of supporting third party services and different families of vNSFs, new vNSFs and analytics can be developed to adapt to new threats.

Data export and sharing - Data export and sharing with 3rd parties

Infrastructure and service attestation - Verification of the integrity of infrastructure and software, prevention of unauthorised modifications

Support for third-party services and vNSFs	1	2	3	4	5	6	7	8	9	Data export and sharing
Support for third-party services and vNSFs	1	2	3	4	5	6	7	8	9	Infrastructure and service attestation
Data export and sharing	1	2	3	4	5	6	7	8	9	Infrastructure and service attestation

Importance of the Performance

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding Performance?

5. Please rate the importance (pairwise comparison) of each one of the Performance factors of a cybersecurity solution

Real Time Monitoring - real-time views and threat visualizations of ongoing threat activity, collect event data in near real time in a way that enables immediate analysis

SECaaS – Security as a service, High Availability of the security solution. Running the whole solution as a service, that allows scalability, redundancy and high availability

Multi-threat support - simultaneous attacks detection & mitigation

Real Time Monitoring	1	2	3	4	5	6	7	8	9	SecaaS
Real Time Monitoring	1	2	3	4	5	6	7	8	9	Multi-threat support
SecaaS	1	2	3	4	5	6	7	8	9	Multi-threat support

Importance of the Business /Strategy aspects

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding Business/Strategy aspects?

6. Please rate the importance (pairwise comparison) of each one of the Business /Strategy aspects of a cybersecurity solution

Capex -> Opex transformation and flexible pricing – Transforming the capital cost to Operational, move competition from HW to SW, lowering the threshold for players to enter the market, Solution with decreased cost, this cost include installation and maintenance, equipment and SW cost, Flexible pricing model, per service, per use case, per data traffic, pay-as-you-go.

Support for new Business Models - New players will enter the market, traditional roles will be changed. Advance applications/services will emerge changing the revenue streams

Compliance to technological Standards - support of open APIs, and standards protocols to be integrated with company systems and tools. Also means data export and sharing capacity in standard formats.

Compliance to data privacy policies (GDPR etc.) - Comply with regulations and standards. No need for separate solutions for compliance, e.g.: privacy, audit and report.

Capex -> Opex transformation and flexible pricing	1	2	3	4	5	6	7	8	9	Support for new Business Models

Capex -> Opex transformation and flexible pricing	1	2	3	4	5	6	7	8	9	Compliance to technological Standards
Capex -> Opex transformation and flexible pricing	1	2	3	4	5	6	7	8	9	Compliance to data privacy policies
Support for new Business Models	1	2	3	4	5	6	7	8	9	Compliance to technological Standards
Support for new Business Models	1	2	3	4	5	6	7	8	9	Compliance to data privacy policies
Compliance to technological Standards	1	2	3	4	5	6	7	8		Compliance to data privacy policies

Importance of the Ease of Use

Which of the following you believe will be the critical factor (pairwise comparison) for SHIELD regarding Ease of Use aspects?

7. Please rate the importance (pairwise comparison) of each one of the Ease of Use aspects of a cybersecurity solution

Built-in templates and workflows - content management, management, event handling, use cases workflow to support incident response, Out-of-the-box use cases covering a variety of use cases, such as user activity monitoring, network monitoring, data exfiltration and malware activity, automation and out-of-the-box content, operational use cases (like templates).

Scalability/ Modularity - expandability of the platform, just by adding hardware resources. Ability for modular/incremental deployment.

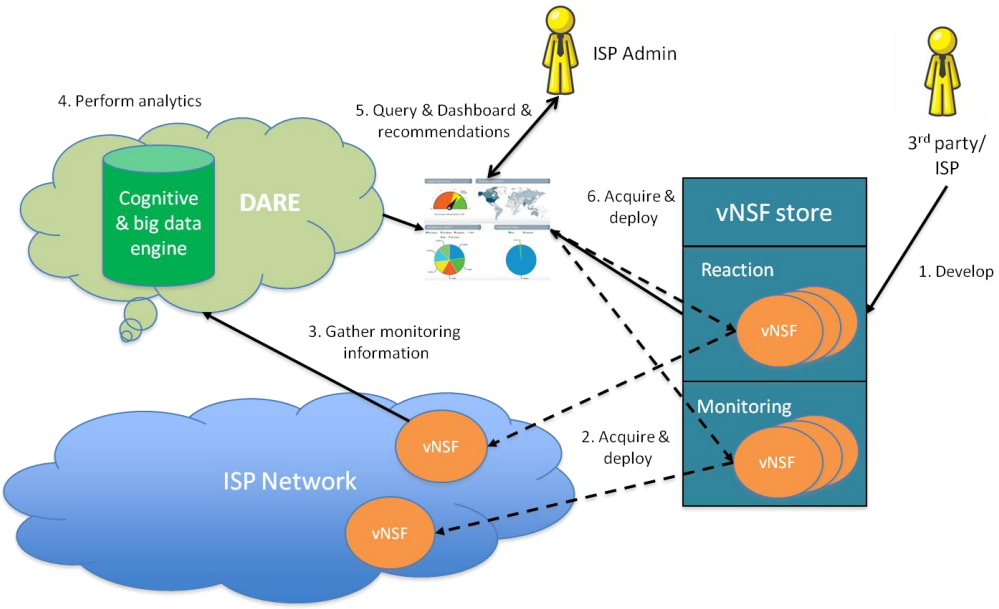
Deployment and Support Simplicity – Easy setup, operations and maintenance; support for non-expert users.

Built-in templates and workflows	1	2	3	4	5	6	7	8	9	Scalability/Modularity
Built-in templates and workflows	1	2	3	4	5	6	7	8	9	Deployment and Support Simplicity
Scalability/ Modularity	1	2	3	4	5	6	7	8	9	Deployment and Support Simplicity

Use Cases description

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

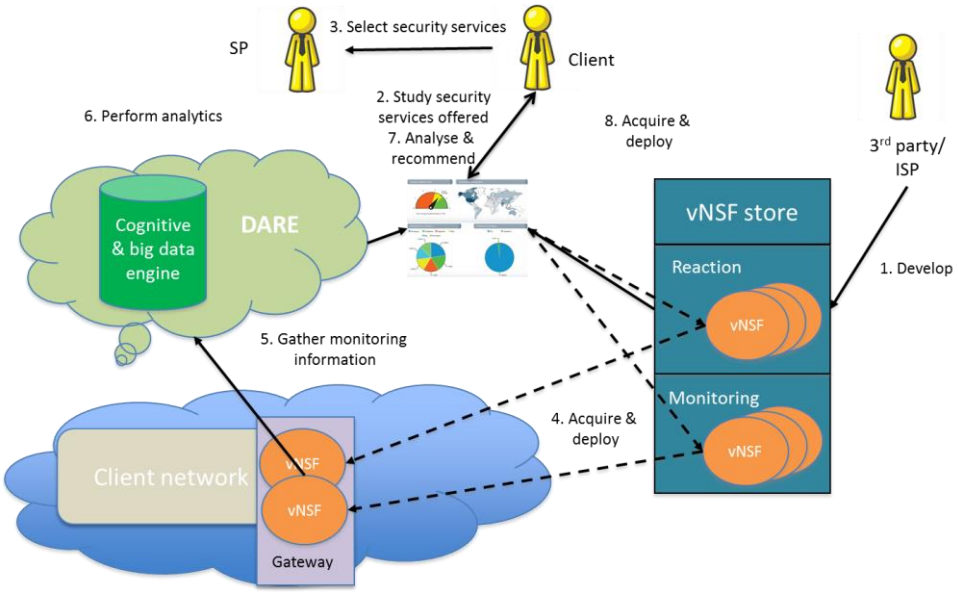
In order to protect their own network infrastructure, ISPs have to deploy specific hardware which is very expensive since this hardware has to be updated and maintained by very specialized operators. The virtualization offered by SHIELD in this use case aims to dramatically reduce this cost by replacing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