Factors Influencing Market Adoption and Evolution of NFV/SDN Cybersecurity Solutions. Evidence from SHIELD Project

D. Katsianis, I. Neokosmidis
INCITES Consulting SARL
Strassen, Luxembourg

A. Pastor
Telefonica I+D
Madrid, Spain

L. Jacquin
Hewlett Packard Labs
Hewlett Packard Enterprise
Bristol, United Kingdom

G. Gardikis
R&D Department
Space Hellas S.A.
Athens, Greece

Abstract— **SHIELD is an EU-funded project, targeting at the design and development of a novel cybersecurity framework, with the aim of which offers security-as-a-Service in an evolved telco environment. The SHIELD framework leverages NFV (Network Functions Virtualization) and SDN (Software-Defined Networking) for virtualization and dynamic placement of virtualised 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 the infrastructure and the services. This paper presents a detail Roadmapping analysis and identifies the factors that will affect market adoption and the evolution of SHIELD or similar cybersecurity solutions.**

Keywords— NFV; big data analytics; infrastructure and service attestation; Fuzzy Analytical Hierarchy Process; market; adoption; business

I. INTRODUCTION

Cybercrime techniques continuously evolve to target victims and to subvert information technology. It is expected that mobility and heterogeneity of devices (including IoT/IoX), as well as Big Data environments, will be two of the main targets for cybercrime in the years to come. Growth in worldwide cloud-based security services remains strong, reaching $5.9 billion in 2017, up 21 percent from 2016, according to [1]. 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. According to IDC [2], public IT cloud services were double and more than $107B in 2017. These services will have an annual growth rate (CAGR) of 23.5%. Software-as-a-Service (SaaS) remains the largest public IT services category, capturing 59.7% of revenues in 2017. PaaS and IaaS are the fastest growing categories (CAGRs of 29.7% and 27.2%).

The priorities of the EC Digital Agenda and Single Market state that protection against online accidents and crime has become central to consumer confidence and the online economy [3]. The success of attacks carries too many negative consequences for the victims, where most of these concerns regard the loss of sensitive data and intellectual property, opportunity costs (including service and employment disruptions), the damage to the brand image and company reputation, penalties (such ones defined in GDPR [4]) and contractual compensations to customers of commercial networks after service disruptions.

SHIELD (Securing against intruders and other threats through an NFV-enabled environment) [5], [6], [7] is an EU-funded project with the ambition to address the above mentioned challenges by designing and implementing an integrated framework for next-generation security-as-a-service (SECaaS) offerings. All these many facets contribute into creating a complex landscape with many possibilities for successful innovation and new business opportunities.

This paper aims to assess and prioritize several crucial technological and socioeconomic issues that are expected to influence the deployment and market adoption of the SHIELD solution in particular and NFV/SDN cybersecurity solutions in general. This evaluation is carried out through a number of surveys conducted using elements of the Fuzzy Analytical Hierarchy Process (Fuzzy AHP) framework [8], and more specifically pairwise comparisons. The obtained results will be a valuable tool for policy and decision makers, in order to accelerate the successful deployment of similar solutions.

The next sections of the paper describe the SHIELD concept, the selected methodology with the criteria used, the results and the conclusions part.

II. THE SHIELD CONCEPT

The SHIELD framework (Fig.1) 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

978-1-5386-1478-5/18/$31.00 ©2018 IEEE

trustworthy cybersecurity solution. It aims at delivering IT security as an integrated service of virtual network infrastructures, which can be tailored for Communication Service Providers (CSPs) 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 offers, vNSFs can be distributed within the network infrastructure particularized to the user/customer needs. This allows to radically optimize resource allocation, minimize costs and reduce incident response time. Data and logs from vNSFs are aggregated and fed into an information-driven Intrusion Detection and Prevention System (IDPS) platform called Data Analysis and Remediation Engine (DARE), featuring analytical components capable of predicting specific vulnerabilities and attacks. The DARE relies on continuous monitoring of the network traffic, using monitoring vNSF, and translates its observations into adversarial options, behaviors and intents.

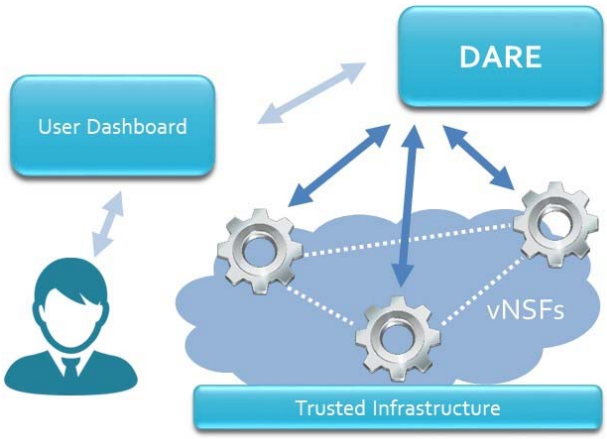

Fig. 1. SHIELD Framework

III. FAHP Methodology and Criteria Selection

A. FAHP Methodology

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 FAHP methodology for the Criteria Comparison Part presented in paragraph B.

AHP [9], [10] 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 pairwise 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], [12], [13] as a means to address this uncertainty. More details about the method and the modelling steps could be found in [13]. Fuzzy numbers are used in order to model the relative importance of criteria and sub-criteria. 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.

B. Formation of the problem

Originally 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, forming the comparison criteria between SHIELD and similar products.

As a result of the selection of the main capabilities, 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 set of factors that will affect market adoption and evolution of SHIELD solution (Fig. 2). In the second level, the criteria (Cr_i), affecting the objective (factors) are determined.

- C_1-Technology Enablers - Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed
- C_2-SIEM (Security information and event management) like functionalities, functionalities like user behaviour analysis, advanced analytics and threat mitigation
- C3-Platform Features – Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation
- C_4-Performance - Performance aspects, such as real-time operation, SECaaS including high availability and multi-threat supportC_5-Business/Strategy aspects - Market related issues and compliance issues
- C_6-Ease of Use - Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity

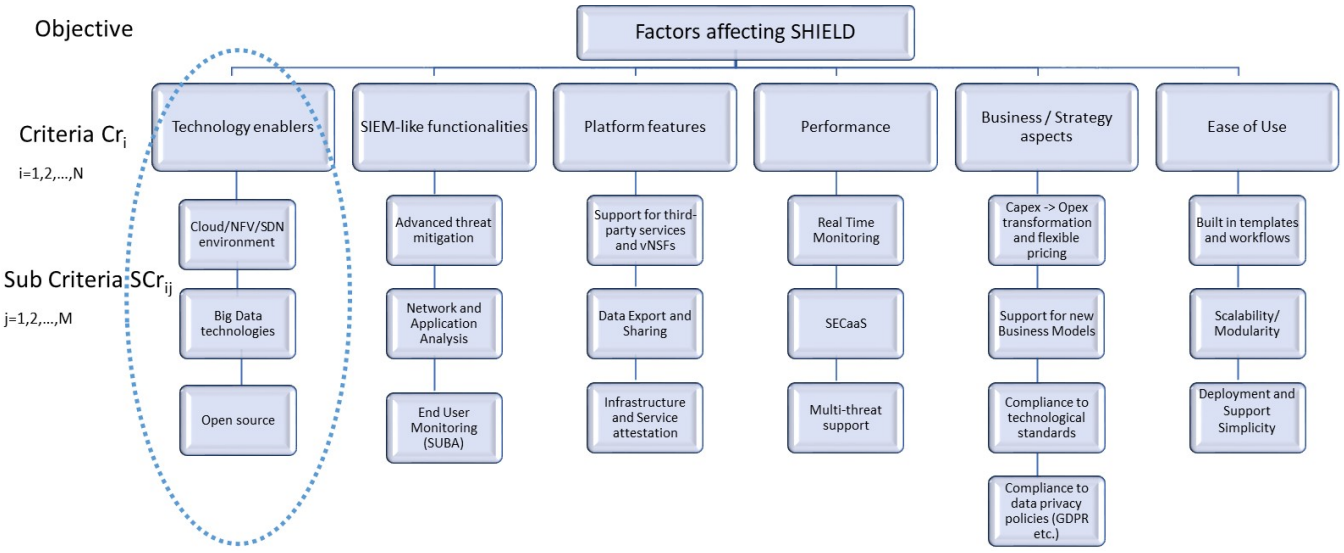

Fig. 2. Multi-level hierarchy of interrelated criteria and sub-criteria

Finally, in the third level, the criteria are further analysed into their relevance sub-criteria (SCr_{ij}). Sub-criteria represent a specific feature characterizing a criterion (Cr_i). Identification of the criteria and their sub-criteria is accomplished based on the focus of their preferential independence. Once the hierarchical structure has been constructed and the criteria and sub-criteria have been determined, appropriate questionnaires are conducted and distributed to experts.

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 I [9].

TABLE I. 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 I 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 stakeholders 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 (70%) and secondly in Business (30%).

The online questionnaires were conducted and completed during a period of 1 month (up 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) [12], enforced the reliability of the results

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

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

IV. Results and Discoussion

A. 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 or similar NFV/SDN solutions. 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 illustrated in Fig 3.

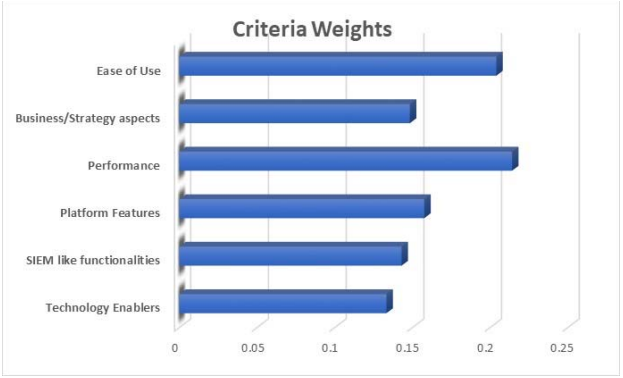

Fig. 3. Relative weights of SHIELD market adoption and evolution criteria

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 (Fig. 3, less than 0.15) 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.

It is also interesting to investigate the ranking of criteria using the fuzzy weights (Fig. 4). 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. Fig. 4 illustrates that there is a large degree of overlapping between the two first (Performance and Ease of Use) the four last criteria (Business/Strategy aspects, SIEM like functionalities, Platform Features, Technology Enablers). This is a clear indication that the ranking of these criteria may possibly change (a situation referred to as rank reversal) among the two first and between the other ones, especially when the solutions will become more mature.

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 less important considerations in the deployment for similar solutions like SHIELD but the order can change because of the overlapping.

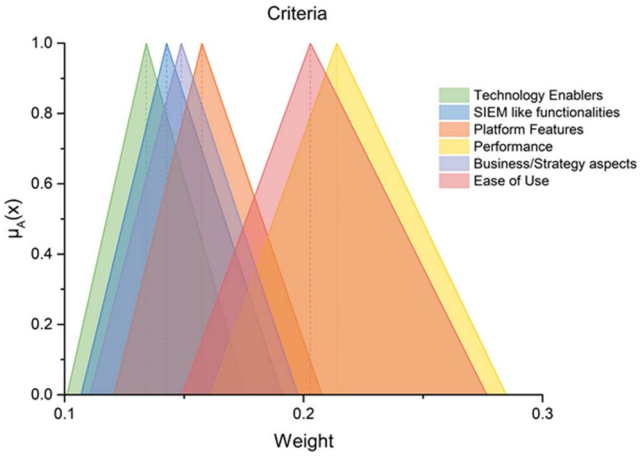

Fig. 4. Fuzzy evaluation of Criteria

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.

B. 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). The results presented in both the previous section and Table II 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 similar solutions should be elaborated with SECaaS including high availability, deployments simplicity and with advanced features. Global Priorities of sub-criteria

On the contrary less important are: End User Monitoring/SUBA(Security UBA [15]), 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. This is a major barrier for the adoption of new players since the trust on the vendor and vendor lock in are barriers for all new solutions.

TABLE II. GLOBAL PRIORITIES OF SUB-CRITERIA

(SCr_{ij})	Sub-criteria	Global Priority
SCr_{63}	Deployment and Support Simplicity	9.50%
SCr_{33}	Infrastructure and service attestation	9.10%
SCr_{42}	SECaaS	8.40%
SCr_{41}	Real Time Monitoring	7.30%
SCr_{21}	Advanced threat mitigation	7.10%
SCr_{62}	Scalability/ Modularity	7.10%
SCr_{11}	Cloud/NFV/SDN Environment	6.50%
SCr_{54}	Compliance to data privacy policies (GDPR [4] etc.)	6.30%
SCr_{43}	Multi-threat support	5.60%
SCr_{22}	Network & application analysis	5.00%
SCr_{31}	Support for third party services and vNSFs	4.80%
SCr_{12}	Big Data technologies	3.90%
SCr_{61}	Built-in templates and workflows	3.90%
SCr_{53}	Compliance to technological Standards	3.30%
SCr_{51}	Capex -> Opex transformation & flexible pricing	3.10%
SCr_{13}	Open source	3.00%
SCr_{23}	End User Monitoring/SUBA	2.20%
SCr_{52}	Support for new Business Models	2.10%
SCr_{32}	Data export and sharing	1.90%

V. CONCLUSIONS

This paper presents critical roadmapping results for the adoption of similar cybersecurity solutions like SHIELD. The factors that will affect cybersecurity solutions and deployment as well as and market adoption were initially identified and prioritized. The results collected via an online survey contributed to produce some factors, which is well aligned to both the market needs and the recent trends in NFV architectures and big data analytics as well as SIEM completive tools.

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 investing in similar criteria with the contacted survey. 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. The findings of this study can be an important tool for decision and policy makers in the cybersecurity NFV/SDN area in order to accelerate similar solutions.

ACKNOWLEDGMENT

The work described in this article has received funding by the European Union Horizon 2020 research and innovation programme, under Grant Agreement no. 700199.

REFERENCES

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

[2] IDC, available online https://softwarestrategiesblog.com/tag/cloud-computing-forecasts

[3] European Commission, “Digital Agenda for Europe”, Nov. 2014, available online at http://europa.eu/pol/pdf/flipbook/en/digital_agenda_en.pdf

[4] The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) directive

[5] EU SHIELD project, (Securing against intruders and other threats through an NFV-enabled environment) https://www.shield-h2020.eu/

[6] G. Gardikis et al., "SHIELD: A novel NFV-based cybersecurity framework," 2017 IEEE Conference on Network Softwarization (NetSoft), Bologna, 2017, pp. 1-6.

[7] S. Y. Zhu, S. S. Hayward, L. Jacquin, R. Hill,, Guide to Security in SDN and NFV, in book, Springer, 2017

[8] Da-Yong Chang, Applications of the extent analysis method on fuzzy AHP, European Journal of Operational Research, Volume 95, Issue 3, 1996, Pages 649-655,ISSN 0377-2217,

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

[13] 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.

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

[15] User Behavior Analytics,available online https://www.gartner.com/doc/2831117/market-guide-user-behavior-analytics