A UNIVERSAL SECURITY INFRASTRUCTURE FOR ISPS AND CORPORATE NETWORKS BY USING NFV-ENABLED TECHNOLOGIES: THE SHIELD PROJECT

SHIELD exploits NFV for adaptive monitoring of an IT infrastructure and for feeding the data to an analytics engine to detect attacks in real time. An intelligent reaction system is then activated to reconfigure the SDN/NFV infrastructure so that the attacks are thwarted. The SDN/NFV infrastructure itself is protected from attacks thanks to trusted computing techniques that permit to quickly identify misbehaving nodes.

During the last leg of the project, SHIELD has released the final version of the platform prototype, which is available at the official Github account: https://github.com/shield-h2020. In addition, the conclusions of the technical development work, along with the final architectural design, have been published in deliverables and are available at the project website: https://www.shield-h2020.eu/documents/project-deliverables.html.

The SHIELD consortium has participated to several dissemination events to maximise the impact of the project results within both scientific and industrial communities. The consortium has been invited to present the project results during the Software Defined Networks Security workshop at **CODE-2018**, organised by ENISA in Munich (Germany) on July 11st 2018. The project held a panel session on Collaborative info-sharing on September 27th 2018 within the CyberTech 2018 event in Rome (Italy). A presentation of the SHIELD architecture and of its demonstrations was given at the InfoCom World 2018 industrial event in Athens (Greece) on November 21st 2018, within a dedicated session on EU funded projects' results. SHIELD participated to the **ICT 2018: Imagine Digital** event, organised by the European Commission in Vienna (Austria) on 4-6 December 2018. The event focused on the European Union's priorities in the digital transformation of society and industry, and SHIELD presented a networking session named Big Data & Machine Learning for network security: approaches and benchmarks on December 5th, 2018. Finally, SHIELD will participate to the H2020 Project Clustering Workshop organised by the GHOST project on March 28th, 2019.

With respect to standardisation activities, the consortium participated at the **Trusted Computing Group** annual members meeting in Lisbon (Portugal) on October 16th 2018 to present the SHIELD project and its use of Trusted Computing technologies and mechanisms to enhance security of virtualised infrastructures. Moreover, a *Proof of Concept* on network management security, leveraging the SHIELD intelligent reaction system, was presented at the **ETSI** *Experiential Network Intelligence* (ENI) working group in Leganes (Spain) on 3-5 December 2018.

The paper entitled *"Application of distributed computing and machine learning technologies to cybersecurity"* has been presented to the Computer & Electronics Security Applications Rendez-vous (**C&ESAR 2018**) conference in Rennes (France), on 19-21 November 2018. The Future Generation Computer Systems (Elsevier) journal has accepted the paper *"Integrity verification of Docker containers for a lightweight cloud environment"*, whose publication is expected in Volume 97 (August 2019).

During this period, the consortium has participated to the organisation of scientific workshops as well. The 1st International Workshop on Cyber Threat Intelligence Management (**CyberTIM 2018**) has been co-organised by the

European Commission | Horizon 2020 European Union funding for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700199

SHIELD, PROTECTIVE and C3ISP projects in conjunction with the ARES 2018 conference in Hamburg (Germany), on 27-30 August 2018. Moreover, SHIELD is co-organising the 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (**SecSoft 2019**) together with other EU Cyber-security and 5G projects, namely ASTRID, SPEAR, CYBER-TRUST, REACT and 5GENESIS.

The SHIELD consortium has organised several communication events to showcase the final version of the platform prototype and demonstrate its performance and functionality in realistic scenarios. First, a tutorial entitled *"Modern Network-based Security: Softwarized Networking, Trusted Computing, and Artificial Intelligence for Cybersecurity"* has been organised within the 5th International Conference on Information Systems Security and Privacy (**ICISSP 2019**) on 23-25 February 2019 in Prague (Czech Republic). This tutorial aimed at introducing modern network technologies (Software Defined Networking, and Network Function Virtualization) and then show how to use them along with Trusted Computing, Machine Learning, and Artificial Intelligence techniques to create a trusted protection infrastructure to effectively counter cyberattacks. The technical aspects were complemented by a market and economic analysis, to evaluate benefits versus costs, and by a live showcase of project demonstrations. Within the same event, SHIELD has presented the ETSI ENI PoC in a dedicated booth for the entire duration of the conference. SHIELD has run an exercise based on an enterprise use case together with internal personnel coming from different departments and business units of Telefónica, including technical operational staff, on 7th March 2019. Valuable feedback and recommendations have been provided, including an initial definition of commercial models, network integration and standardisation needs. In parallel, Space Hellas conducted an internal pilot, using the SHIELD technologies in the company's operational network infrastructure, with quite promising results, as assessed by cybersecurity experts during an internal workshop held on March 5th, 2019. Finally, the CESICAT cybersecurity agency has been involved in a pilot that showcased the SHIELD capability to extract statistics regarding network anomalies in an ISP infrastructure on 11th March 2019.

The SHIELD project has participated to the organisation of the *European Network for Cybersecurity* (**NECS)** Winter School 2019 in cooperation with C3ISP EU project, AEGIS and the CINI Cyber Security National Lab, from 18 to 22 February 2019 near Trento (Italy). Within this event, SHIELD has contributed with three theoretical lectures on the key pillars of the project, namely Network Function Virtualization, Artificial Intelligence and Trusted Computing, and a practical session comprising project demonstrations and a hands-on session on Machine Learning application to cybersecurity. Full details of the school program, along with the lectures' material and pictures, are available on the official website.

All the demonstration videos are available through the **EU SHIELD project** YouTube channel, along with a brief overview of the project goals.

https://www.shield-h2020.eu/
@shield_h2020
SHIELD EU Project
info@shield-h2020.eu

European Commission | Horizon 2020 European Union funding for Research & Innovation
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700199