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

The recently launched EU-funded SHIELD project proposes a universal solution for the dynamic establishment and deployment of virtual security infrastructures into ISP (Internet Service Provider) and corporate networks. SHIELD builds on the huge momentum of *Network Functions Virtualisation* (NFV), as currently standardised by ETSI, 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, as defined by *Trusted Computing* (TC).

Data and logs are aggregated and fed into an information-driven *Intrusion Detection and Prevention System* (IDPS). This platform is called *Data Analysis and Remediation Engine* (DARE) and it features analytical components capable of predicting specific vulnerabilities and attacks by analysing the network and understanding the adversary possibilities, behaviour and intent.

The SHIELD virtual security infrastructure can either be used by an ISP for network monitoring and protection, but it can also be offered as-a-service to the ISP clients. For this purpose, SHIELD establishes a catalogue of available virtual security functions from which the ISP clients can select the ones that best match their needs and deploy them to protect their infrastructure. This approach promotes openness and interoperability of security functions and offers an affordable, zero-CAPEX security solution for citizens and SMEs. Moreover, SHIELD services can be easily scaled up or down, configured and upgraded according to clients' needs, as opposed to security solutions based on monolithic hardware.

The SHIELD framework brings together all actors in the security value chain/network (ISPs, enterprises, end users, cybersecurity agencies, security vendors) into a single ecosystem and facilitates the interactions between them, enabling new business models. SHIELD security services can be either used internally by the network operators/ISPs, and/or offered as-a-Service to their clients.

In this initial phase, the partners of the consortium have contributed in the dissemination activities. First, an official web site has been activated, where the relevant information about the project's mission, official documentation and news can be found and are constantly updated. In addition, the SHIELD project is present on different social media (LinkedIn, Twitter), whose channels are used for communication activities.

Given the broad scope of technologies involved in the project, various aspects of the SHIELD concepts have been presented to the scientific and industrial communities in national and international forums. Links to downloadable content (e.g. presentations, posters) can be found here.

A poster describing the general scope of the project has been presented in **the 7th Infocom Security Conference** in Athens (Greece) in March 2017.

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

Regarding the data analytics, the binomial between cybersecurity and Big Data foreseen by the project has been presented at the **Big Data Value Association** (BDVA) General Meeting in Valencia (Spain) in November 2016.

The contribution of SHIELD in the cybersecurity area has been presented to different security-oriented forums. First, the possible application of the SHIELD infrastructure to security of *Internet of Things* (IoT) fleets has been proposed at the audience of the **C&ESAR 2016** conference, held in Rennes (France) in November 2016, which gathers several governmental agencies, industrial leaders, and academic researchers across the country. Additionally, the concepts between SHIELD have been presented in the **CTS 2017** event in Rome (Italy) in April 2017, which focused on cybersecurity issues with IT administrators for Public Sector and decision-makers, attracting a lot of attention.

A paper titled "SHIELD: A Novel NFV-based Cybersecurity Framework", presenting the key use cases and requirements for the SHIELD system and its high-level architectural approach, has been accepted in the Second International Workshop on Security in NFV-SDN (**SNS 2017**) that will be held in conjunction with the IEEE Conference on Network Softwarization at Bologna, Italy.

Regarding the contribution of SHIELD in the NFV environment, a technical solution towards performing software integrity assessment of virtual security functions based on lightweight virtualisation has been presented at the **ETSI NFV-SEC** meeting, held in Bilbao (Spain) on February 21-24, 2017. Also, use cases defined in SHIELD has been accepted as part of the standardization document in an updated version (ETSI NFV 001) that covers new relevant use cases. In addition, the binomial between cybersecurity and network function virtualisation foreseen by the SHIELD concept has been discussed in the **MPLS+NFV+SDN World Congress** from 21st to 24th of March 2017, in Paris (France).

You can find additional information about

- Key user and system requirements collected and defined
- Requirements survey with the participation of security professionals
- High-level system architecture drafted

at:

- Deliverable D2.1 Requirements, KPIs, design and architecture
- Deliverable D6.1 Project Dissemination and Communication Plan

Contact us at info[at]shield-h2020.eu

Visit us at https://www.shield-h2020.eu

Follow us on Twitter @shield_h2020

Connect with us LinkedIn SHIELD EU Project

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