

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 past months, SHIELD released the second edition of the architectural documents and technical specifications for the data analytics engine as well as the NFV platform. The documents are publicly available at the project website: <https://www.shield-h2020.eu/documents/project-deliverables.html>

The SHIELD consortium has submitted proposals for both a networking session and an exhibition/booth at the **ICT-2018 event**, organised by the European Commission on December 2018 in Vienna. In this context, the SHIELD consortium will aim to organize a workshop for showcasing the final prototype of the project.

The SHIELD project will contribute to the organisation of the European Network for Cybersecurity (**NECS**) Winter School in February 2019.

The SHIELD project has been part of the [European Conference on Networks and Communications \(EuCNC 2018\)](#), held in Ljubljana (Slovenia) on June 18-21. In this occasion, the project has participated with a dedicated booth for [demonstration](#) and by co-organising the [Next generation network systems security Workshop](#) with more than 40 participants. The scientific paper “*Factors Influencing Market Adoption and Evolution of NFV/SDN Cybersecurity Solutions. Evidence from SHIELD project*” has been presented in EuCNC 2018 within [APP1 – Key technologies for application areas track](#).

Moreover, the project has been presented at the [Cyber Security Workshop](#), organised in Athens (Greece) on March 20 by the **SAINT** project. SHIELD project has been presented in the [H2020 Project Clustering workshop for demonstrations](#), organised by the project **ReCRED** on April 20th 2018, in Athens. SHIELD contributions in middleboxes’ security have been presented at the [ETSI Security Week](#), held in Sophia Antipolis (France) on June 11th to 15th June 2018.

The scientific contributions of the SHIELD project are discussed in papers submitted to international conferences. The paper entitled “*Container-based design of a Virtual Network Security Function*” has been presented to the [IEEE Conference on Network Softwarization \(NetSoft 2018\)](#), held in Montreal (Canada) on June 25th to 29th. Two scientific papers, entitled “*Evaluation of Apache Spot’s machine learning capabilities in an SDN/NFV enabled environment*” and “*The Mouseworld, a security traffic analysis lab based on NFV/SDN*” have been accepted for publication at the [1st International Workshop on Cyber Threat Intelligence Management](#), held in conjunction with the **ARES 2018** conference in Hamburg (Germany) on August 27th to 30th.



All the demonstration videos from EuCNC 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