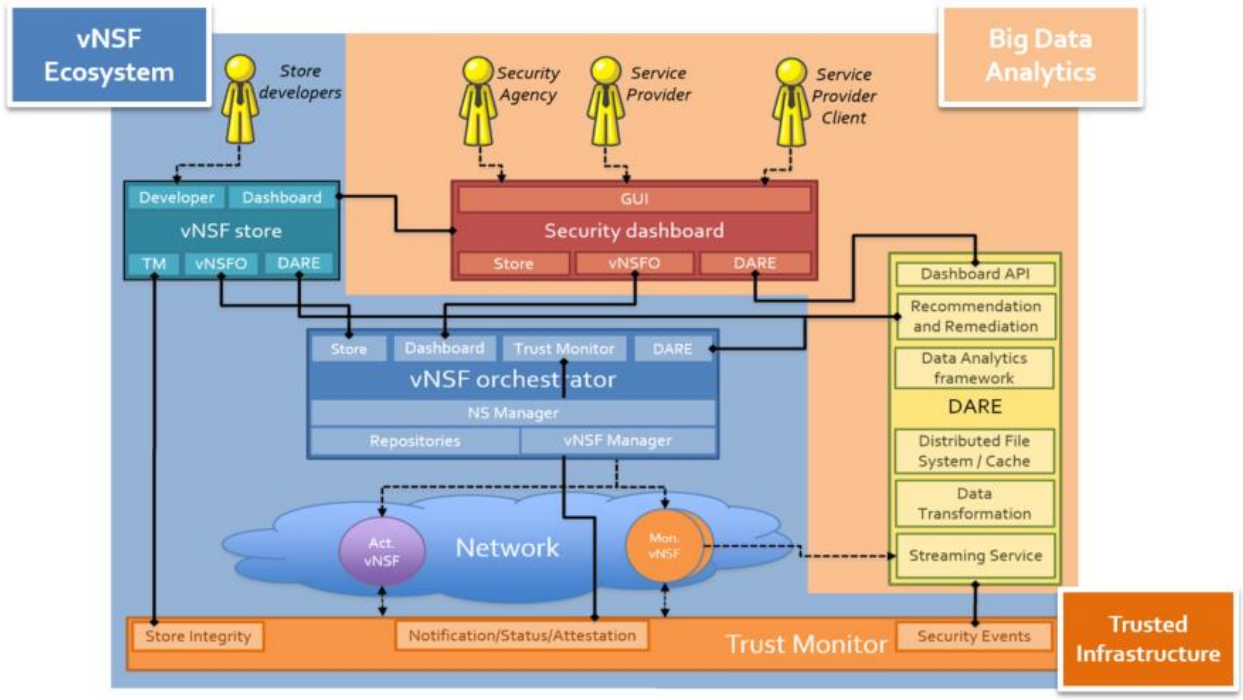
A UNIVERSAL SECURITY INFRASTRUCTURE FOR ISPS AND CORPORATE NETWORKS BY USING NFV-ENABLED TECHNOLOGIES: THE SHIELD PROJECT

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.

The consortium has focused lately on the development of a first prototype of both the vNSF ecosystem and the DARE (Data Analysis and Remediation Engine), depicted in the picture below. The current release of the framework is available on Github.



In this phase, a preliminary integration of these components has been addressed as well, leading to the showcase of three demonstrations:

- **Detection of data exfiltration:** SHIELD uses (and contributes to) the Apache Spot analytics framework. This demo showcases how DNS tunnelling can be used for data exfiltration, how it is detected by Spot and how the Recommendation and Remediation engine produces the rules to block further data exfiltration.

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

- **Detection and mitigation of Distributed Denial of Service attacks:** This end-to-end demonstration showcases how vNSFs can be on-boarded. When a Distributed Denial of Service attack is detected by DARE, the recommendation engine sends the appropriate mitigation rules to the user's dashboard. The rules are then applied by the active vNSF and the attack traffic is dropped.

- **Trust monitor and SDN/NFV attestation:** This demonstration shows how SHIELD detects compromised components of its infrastructure (e.g. SDN switches, the SDN controller, vNSFs).

The project objectives and research outcomes have been presented at the **OPTIMA 2017** conference, organised by the Hellenic Army Academy in Athens (Greece), May 25-26, 2017. The Telefonica **blogthinkbig.com** open research blog has published a public post introducing the SHIELD project on June 29, 2017.

A paper entitled "*SHIELD: A Novel NFV-based Cybersecurity Framework*" was published and presented at the 3rd IEEE Conference on Network Softwarisation (**NetSoft 2017)**, held in Bologna (Italy), July 3-7, 2017. The paper focuses on the SHIELD concepts, use cases, requirements and the overall high-level architecture. Moreover, a paper entitled "*On the establishment of trust in the cloud-based ETSI NFV framework*" has been accepted for publication and presented at the 3rd IEEE International Workshop on Security in NFV-SDN (**SN-2017**), held in conjunction with the IEEE Conference on Network Function Virtualisation and Software Defined Networks (**IEEE NFV-SDN 2017**) in Berlin (Germany), November 6-8, 2017. The paper focuses on the open issues in enabling trust in a NFV environment and proposes an architecture that leverages a cloud attestation framework to be integrated with the NFV ecosystem.

The consortium has accomplished dissemination activities to promote the platform demonstrations as well. The Distributed Denial of Service attack mitigation scenario has been presented at the **ENISA** workshop *"Bonding EU Cyber Threat Intelligence"*, held in Rome (Italy), October 30-31, 2017. Both the DDoS and attestation demonstrations have been described in a paper, entitled *"NFV-based network protection: the SHIELD approach"*, which has been published and presented at the **IEEE NFV-SDN 2017** conference demo track. In this context, the SHIELD consortium has been awarded with the **Best Demo Award** for the best demonstration showcase.

The project has increased lately its presence in social media. A Research Gate account has been activated, to include all the scientific publications related to the project. Moreover, the demonstration videos are available through the **EU SHIELD project** YouTube channel, along with a brief overview of the project goals.

You can find additional information about

- Design, architecture, specifications and technologies of the vNSF ecosystem in the SHIELD Deliverable D3.1 Specifications, design and architecture for the vNSF ecosystem
- Design, architecture, specifications and technologies of the DARE in the SHIELD Deliverable D4.1 Specifications, design and architecture for the usable information-driven engine
- Consortium plan on standardisation activities Deliverable D6.2 Standardisation Plan
- Consortium report on exploitation activities Deliverable D6.3 Interim Report on Exploitation Activities

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