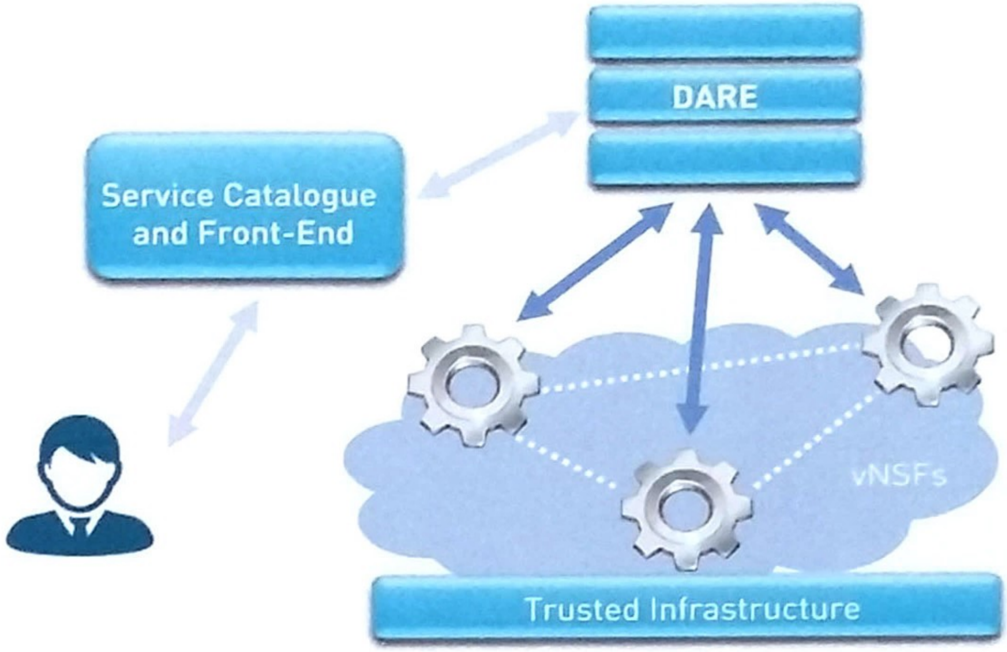
SPACE

SHIELD

Securing against Intruders and other Threats through a NFV-enabled Environment

An Innovative approach to Information Security using Big Data, Threat Monitoring and Machine Learning



- A universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks
- Builds on Network Functions Virtualization (NFV) in order to virtualize security appliances into virtual Network Security Functions (vNSFs)
- Real-time data from vNSFs are aggregated into an information-driven Data Analysis and Remediation Engine (DARE), which leverages state-of-the-art big data storage and analytics in order to detect threats and attacks – and mitigate them
- SHIELD services can be used internally by ISPs and/or enterprises or offered as-a-Service (SecaaS) to customers

SPACE i2cat Hewlett Packard Enterprise inCITES ORION ubiwhere

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

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

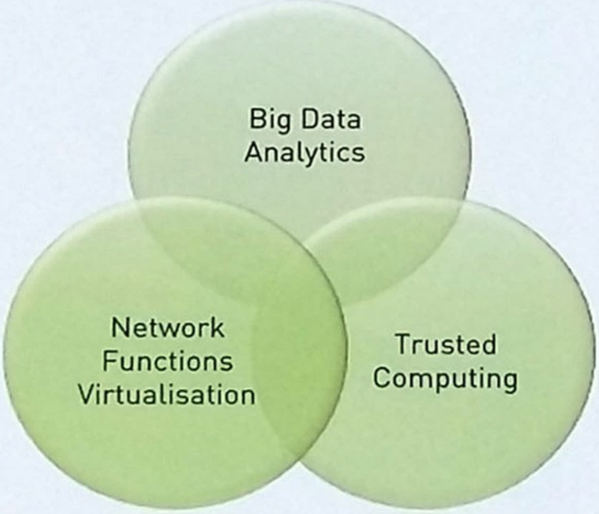
SHIELD

Nowadays, cybercrime is one of the most relevant and critical threats to both the economy and society in Europe. Establishing efficient and effective ways to protect services and infrastructures from ever-evolving cyber threats is crucial for sustaining business integrity and reputation as well as protecting personal and sensitive data.

To that end, the SHIELD project proposes a universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks. SHIELD builds on the huge momentum of Network Functions Virtualisation (NFV), as currently standardised by ETSI, in order to virtualise security appliances into virtual Network Security Functions (vNSFs), to be instantiated within the network infrastructure using NFV technologies and concepts, effectively monitoring and filtering network traffic in a distributed manner.

Logs and metrics from vNSFs are aggregated into a information-driven Data Analysis and Remediatio Engine (DARE), which leverages state-of-the-art bi data storage and analytics in order to predict specifi vulnerabilities and attacks by analysing the networ and understanding the adversary possibilities behaviour and intent.

The SHIELD virtual security infrastructure can eithe used by the ISP internally for network monitoring and protection, but it can also be offered as-a-service to IS customers; for this purpose, SHIELD establishes a "vNSF Store", i.e. a repository of available virtual security functions (firewalls, DPIs, content filters etc.) from which the ISP customers can select the ones which bes match their needs and deploy them to protect thei infrastructure. This approach promotes openness and interoperability of security functions and offers a affordable, zero-CAPEX security solution for citizens and SMEs. Moreover, SHIELD services can be easil scaled up or down, configured and upgraded according to customers' needs, as opposed to security solutions based on monolithic hardware.



Benefits of SHIELD:

- Vendor-neutral Security-as-a-Service offering
- Open and scalable solution
- Fully expandable with third party vNSFs and analytics algorithms
- In-line with emerging technologies and trends
- Suitable for SMEs, big enterprises and ISPs

SPACE