SHIELD

SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT

[H2020 - Grant Agreement No. 700199]

The SHIELD Project

A Brief Overview

ORION INNOVATIONS
Consulting S.A.R.L
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Hewlett Packard Enterprise

SHIELD key facts and figures

Our team

SPACE

i2cat FUNDACIÓ

Hewlett Packard Enterprise

inCITES Consulting S.A.R.L

ΔΗΜΟΚΡΙΤΟΣ

ORION INNOVATIONS PC

POLITECNICO DI TORINO 1859 1906

Telefonica

Telefónica I+D

Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

Talaia NETWORKS

ubiwhere

The motivation for SHIELD

Source: 2016 Norton Report

The motivation for SHIELD

Lack of open-source tools for cybersecurity leveraging massive analytics capabilities

Huge momentum of open technologies for big data

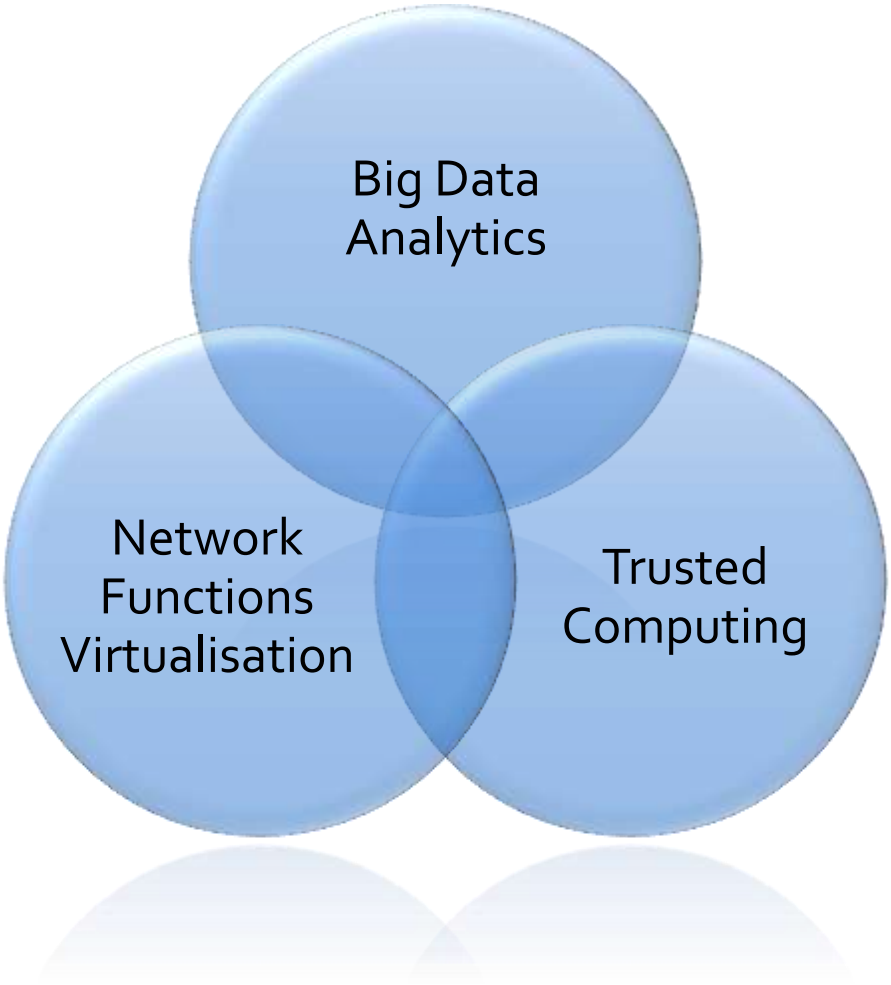
Requirement for expensive, specialized hardware for information security (high CAPEX)

Emergence of the "Security as-a-Service" paradigm, based on cloud and NFV

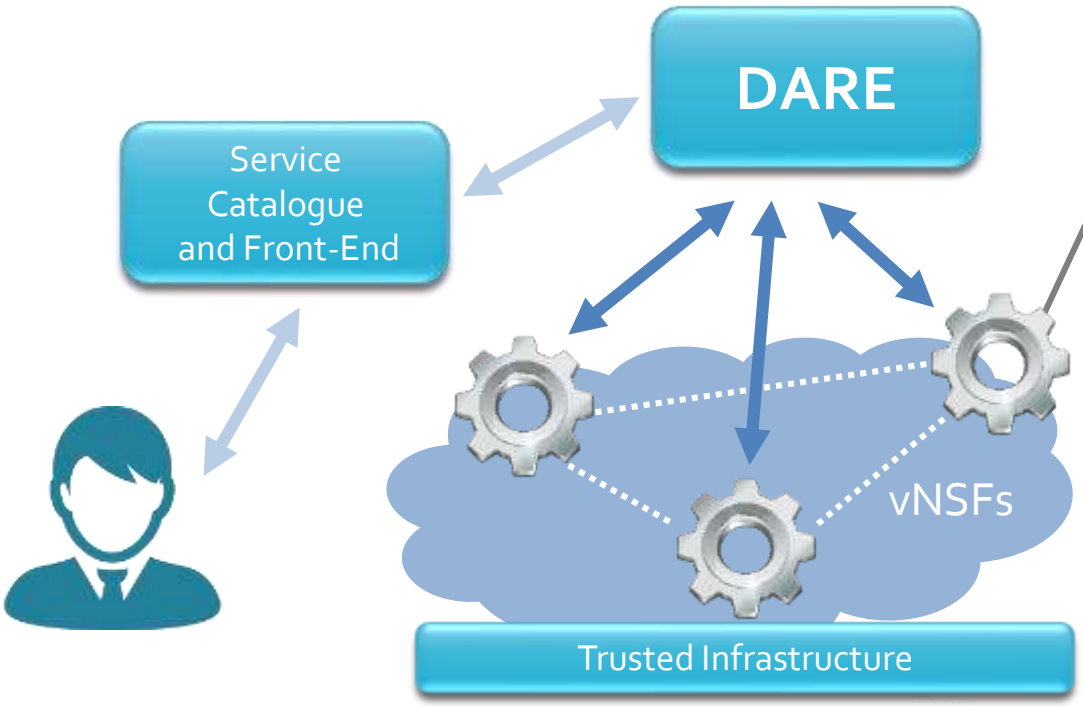
Project mission

SHIELD aims to deliver an open solution for dynamically establishing and deploying virtual security infrastructures in ISP and corporate networks.

The SHIELD concept



The SHIELD system components (I)



KEY TECHNOLOGIES

openstack. OPEN DAYLIGHT Open Source MANO TNOVA sonata

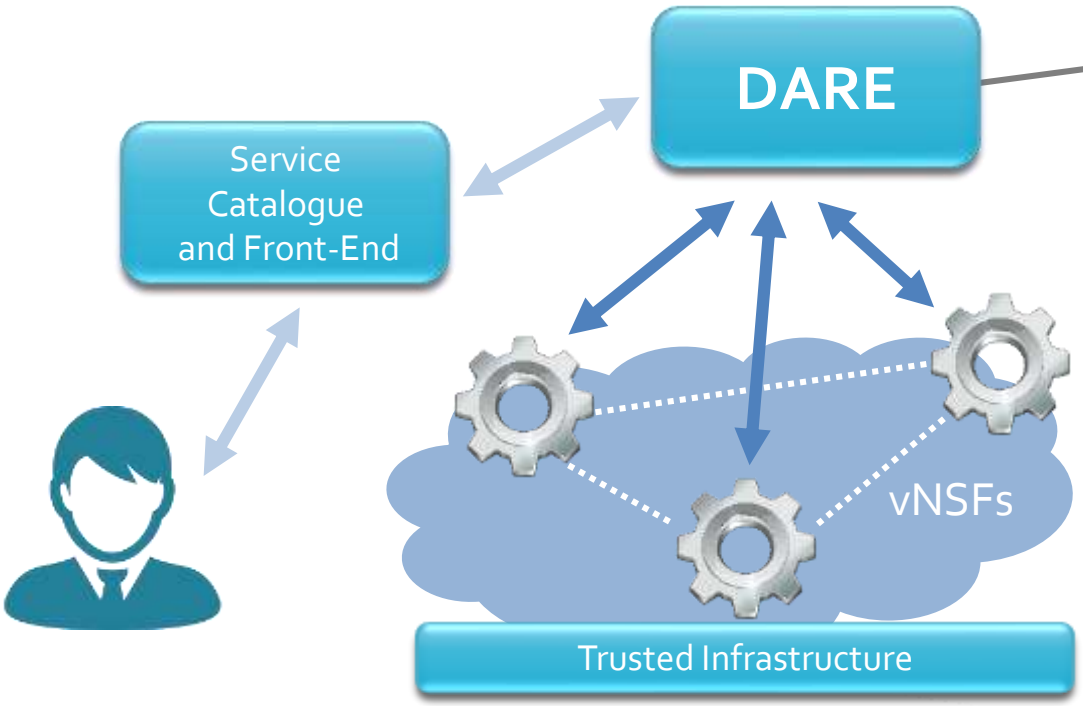
VIRTUAL NETWORK SECURITY FUNCTIONS (VNSFS)

SHIELD offers Security as-a-Service (SecaaS) based on virtualised Network Security Functions (vNSFs).

vNSFs are instantiated within the network infrastructure by a vNSF orchestrator in order to effectively monitor and filter network traffic in a distributed manner.

Advertisement, browsing, selection and trading of vNSFs in a secure manner is provided by a logically centralised repository (Service Catalogue)

The SHIELD system components (II)



DATA ANALYSIS AND REMEDIATION ENGINE (DARE)

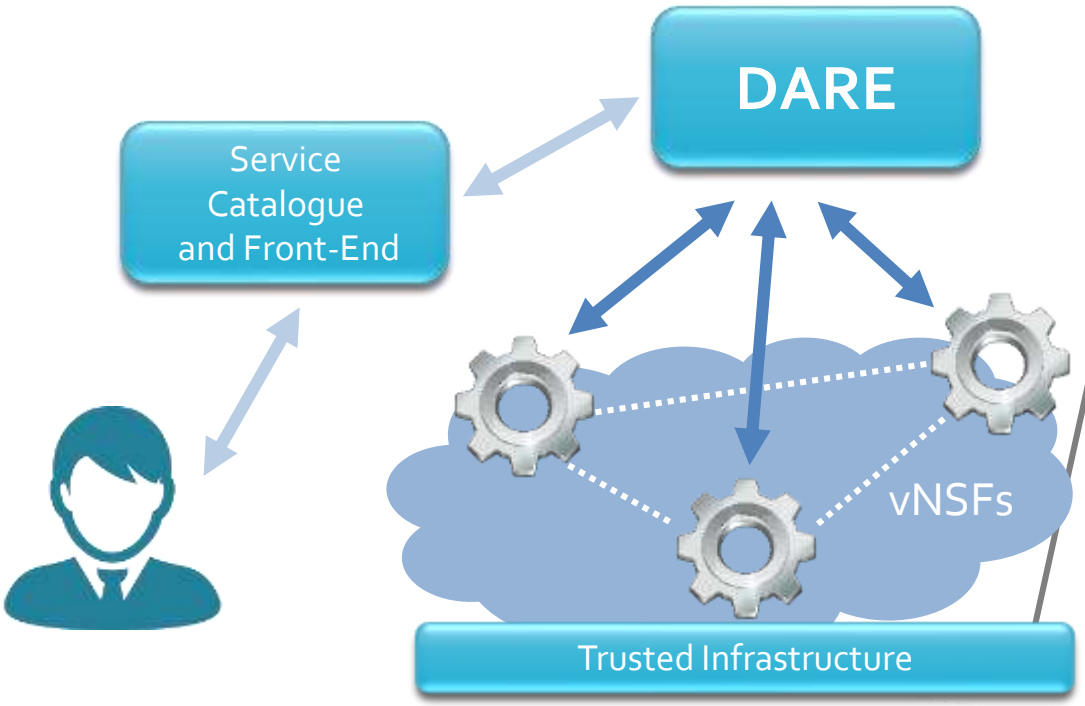
DARE is an information-driven IDPS platform capable of predicting specific vulnerabilities and attacks by relying on Big Data, Threat Monitoring and Machine Learning to analyse the output produced by vNSFs.

Pattern discovery techniques analyse data to identify current malicious behaviours or predict likely threats. Analysis' results are accessible by systems and security administrators via a dashboard.

KEY TECHNOLOGIES

hadoop · APACHE Spark · Apache Spot

The SHIELD system components (III)



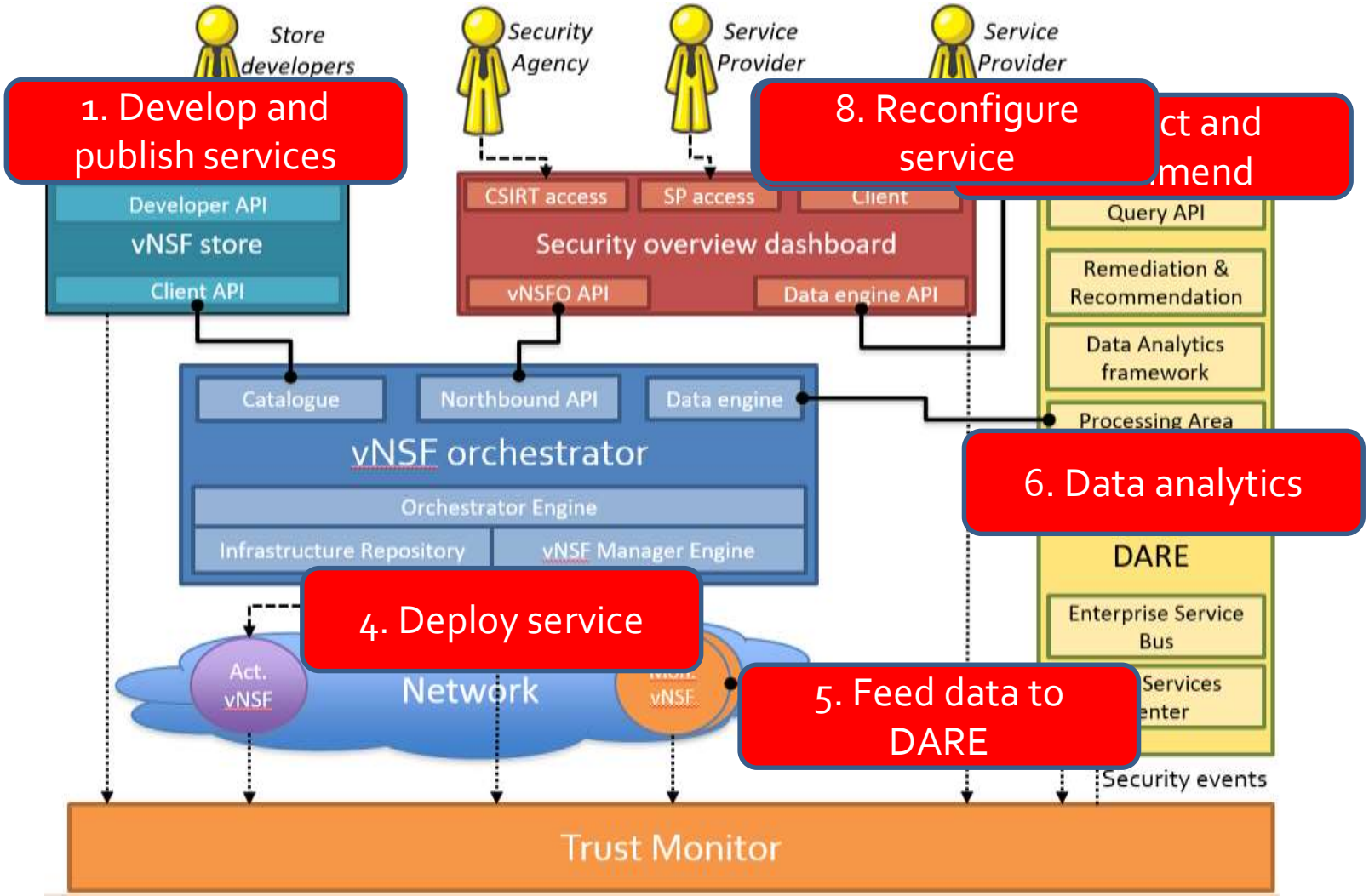
TRUSTED INFRASTRUCTURE

The trustworthiness of the secure SHIELD framework is implemented by relying on Trusted Computing technologies. The infrastructure attestation binds the vNSFs and the network configuration with the store and orchestration of the network.

The key components of the secure SHIELD framework are protected using Trusted Platform Modules (TPM), assuring the integrity of the software and the configuration.

KEY TECHNOLOGIES

UC realization: SECaaS



Key project milestones

Current status

- ✓ User requirements and high-level system architecture updated
  - Publicly available at: https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D2.1_Requirements_KPIs_Design_and_Architecture_v1.0.pdf
- ✓ Detailed architecture and technical specs of subsystems
  - Publicly available at: https://www.shield-h2020.eu/documents/project-deliverables/SHIELD_D4.1_Specifications,_Design_and_Architecture_for_the_Usable_Information-Driven_Engine_v.1.0.pdf
  - https://www.shield-h2020.eu/documents/project-deliverables/SHIELD_D4.1_Specifications,_Design_and_Architecture_for_the_Usable_Information-Driven_Engine_v.1.0.pdf

Check out our latest demos!

EU SHIELD PROJECT

- Project overview: https://www.youtube.com/watch?v=z8b-TQi2fvs
- NFV infrastructure and service attestation: https://www.youtube.com/watch?v=qy-gEq6DYM4
- Detecting and mitigating Distributed Denial-of-Service (DDoS): attacks: https://www.youtube.com/watch?v=a1k5mLfGxkE
- Detecting DNS tunneling with Apache Spot: https://www.youtube.com/watch?v=YxWxaIJW3ho

Follow us!

https://www.shield-h2020.eu/

@shield_h2020

SHIELD EU Project

info@shield_h2020.eu

SHIELD has received financial support from the European Commission under Grant Agreement No. 700199