SHIELD

SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT
[H2020 - Grant Agreement No. 700199]

Description of SHIELD PoC Proposal

ETSI ENI #8 Meeting, Leganés
3-5 Dic. 2018

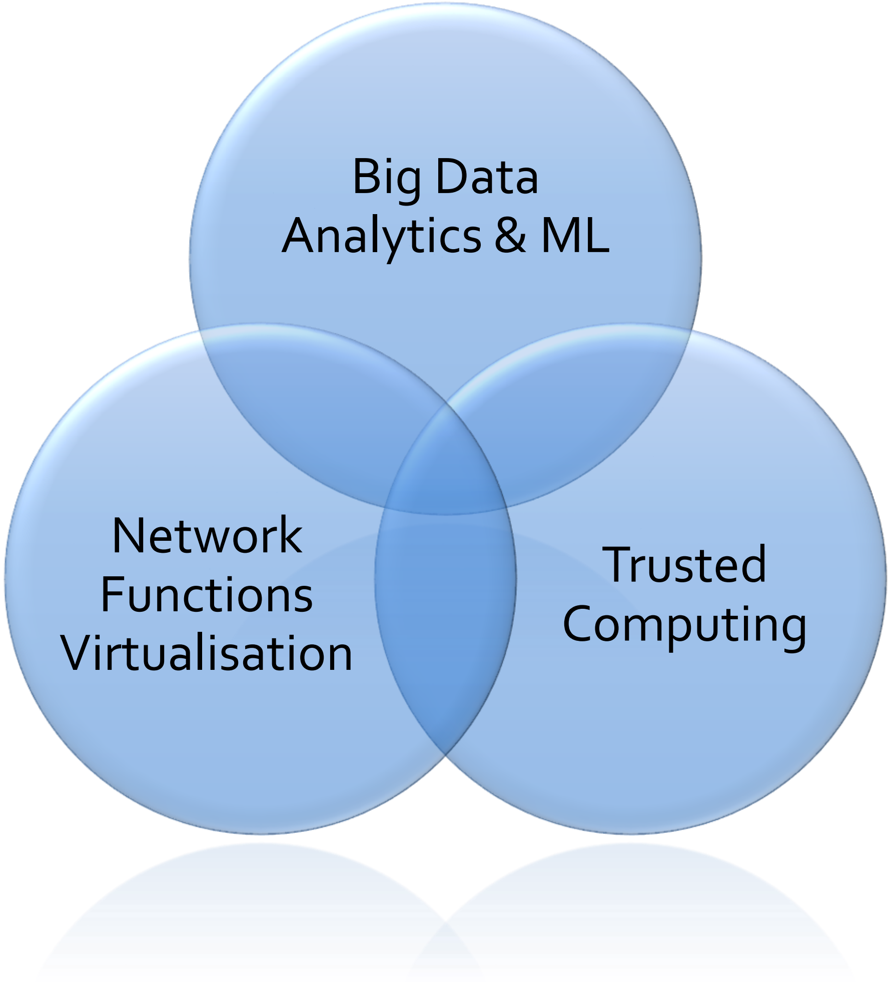
PoC Proposal summary

- Demonstration for a specific use case:
  - Focused on network ***security*** management
- Generalization of use case #2.4: Policy-based network slicing for IoT security
  - Assume any type of attack, not only those to IoT devices
  - Isolation at network layer based on NFV
- Cognitive Management
  - Through Machine Learning support
- Bonus: Trusted computing
  - Attestation capacity for devices that generate metrics
- Prototype created by the SHIELD project (https://www.shield-h2020.eu)

Objectives

- PoC Goal #1: Demonstrate an AI framework able to detect network attacks over NFV network based on the combination of several Machine Learning algorithms
- PoC Goal #2: Present a policy-driven control loop:
  - ML-based attack detection
  - Mitigation recipes through an intent-based security policy
  - Translated & implemented in a NFV environment with security VNFs (vNSF)
- PoC Goal #3: Remote attestation technology to avoid device and data collecting corruption or tampering.

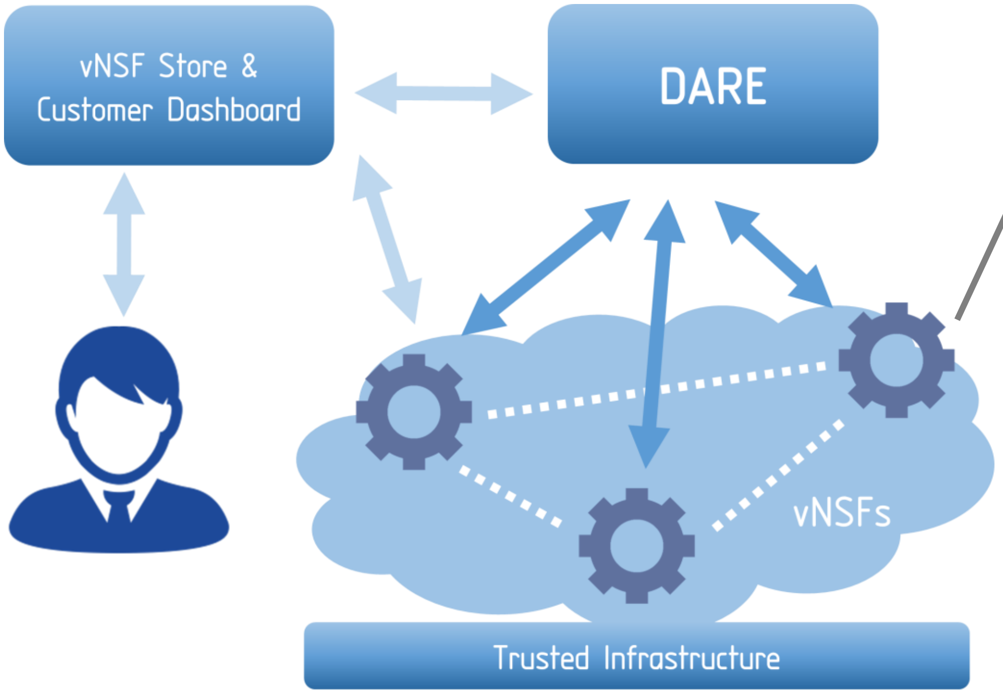
Concept


Big Data Analytics & ML

Network Functions Virtualisation

Trusted Computing

System components (I)



KEY TECHNOLOGIES

openstack. OPEN DAYLIGHT Open Source MANO TNOVA sonata

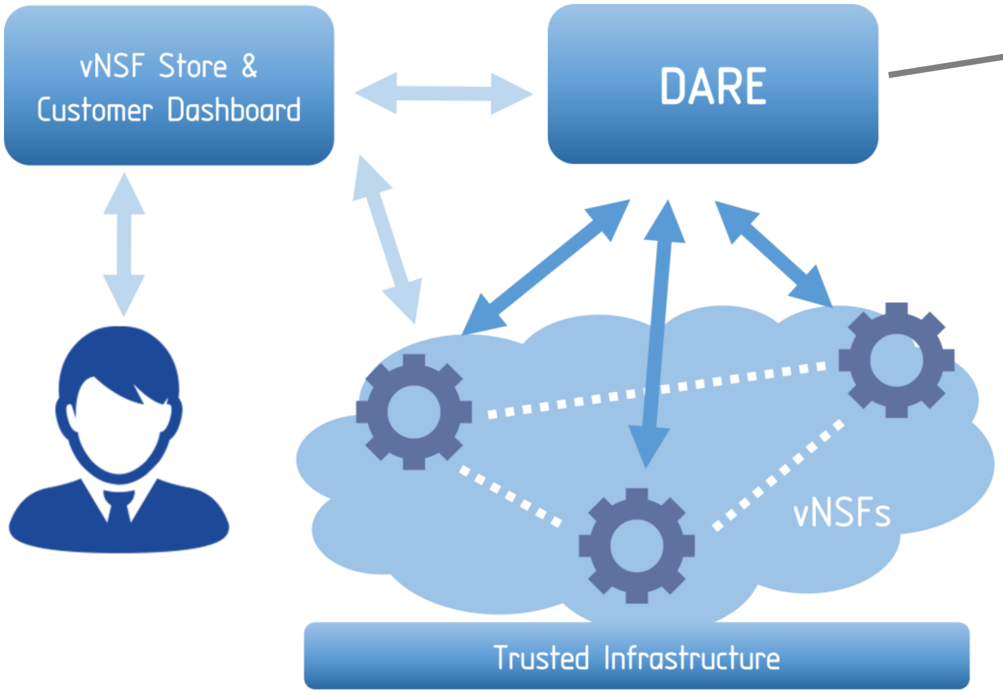
Virtual Network Security Functions (vNSFs)

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)

System components (II)



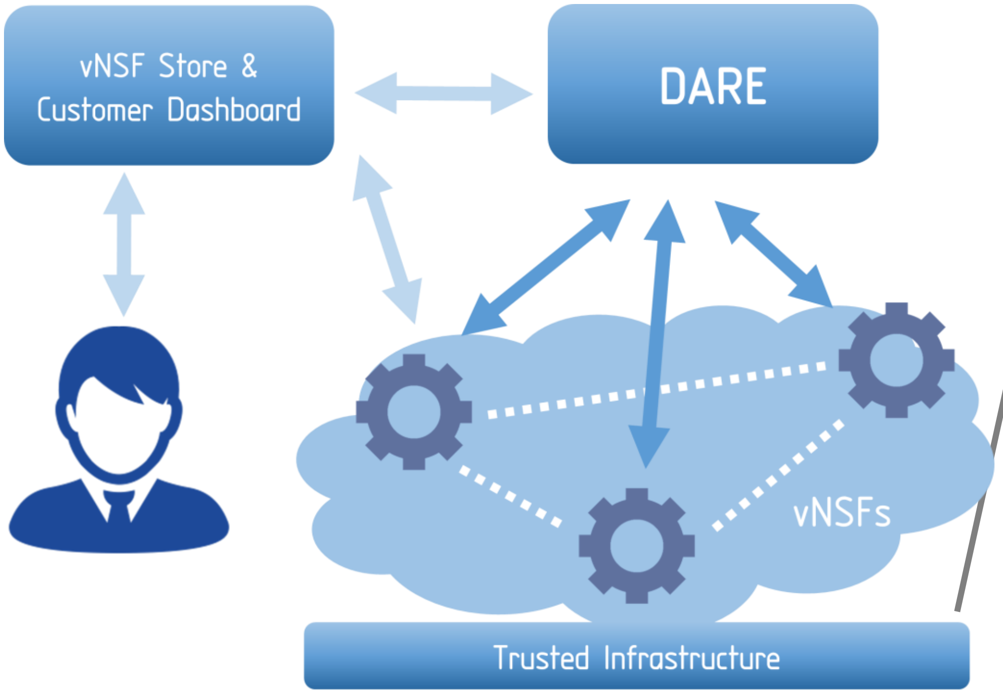
KEY TECHNOLOGIES

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.

System components (III)



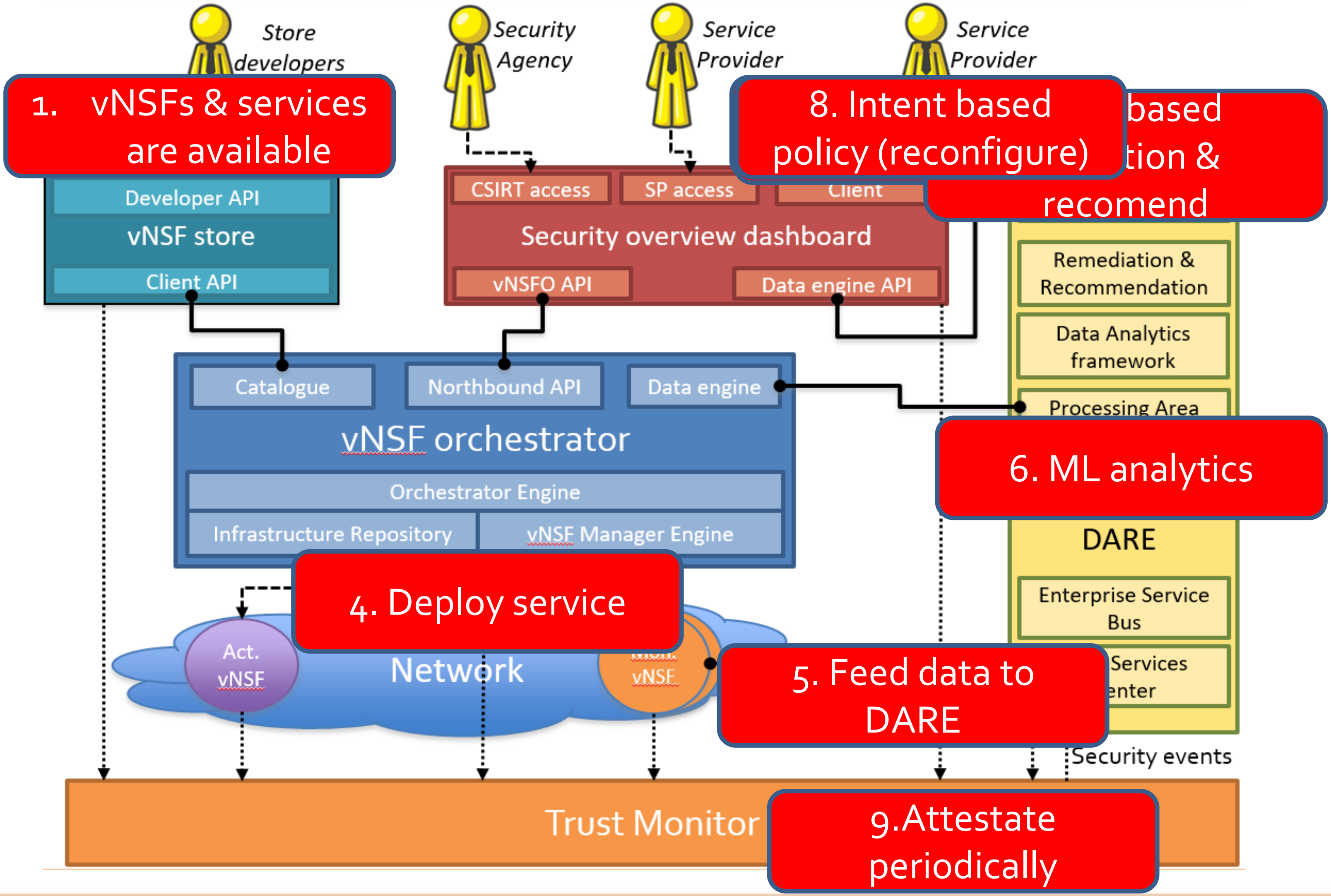
KEY TECHNOLOGIES

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.

PoC in action



1. vNSFs & services are available

8. Intent based policy (reconfigure)

based
tion &
recomend

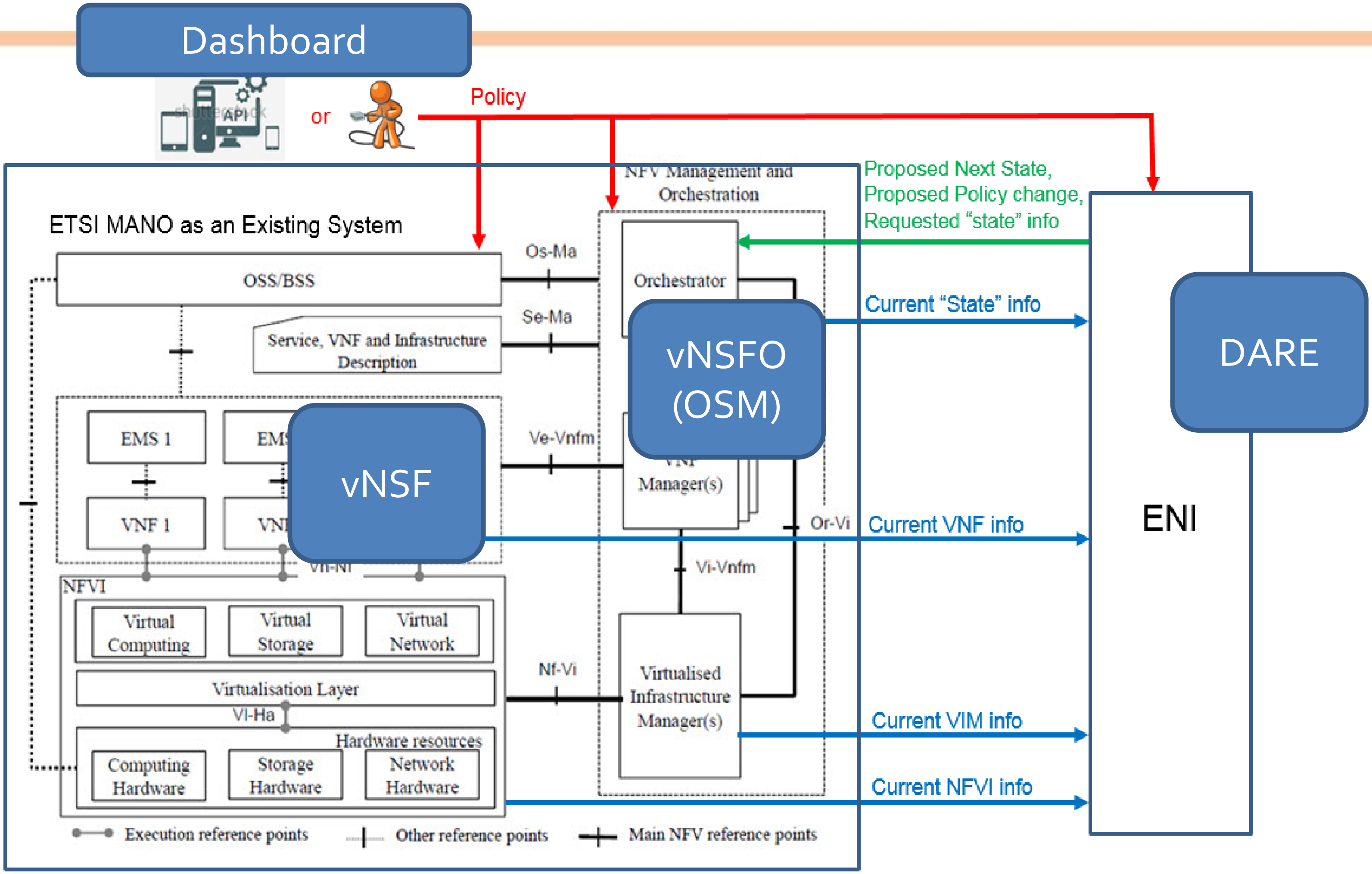
6. ML analytics

4. Deploy service

5. Feed data to DARE

9.Attestate periodically

Interaction between the NFV MANO and ENI



Dashboard

API or

Policy

ETSI MANO as an Existing System

NFV Management and Orchestration

OSS/BSS

Os-Ma

Se-Ma

Service, VNF and Infrastructure Description

Orchestrator

vNSFO (OSM)

EMS 1

EMS

VNF 1

VNF

vNSF

Ve-Vnfm

VNF Manager(s)

Or-Vi

Vi-Vnfm

Vn-Nf

NFVI

Virtual Computing

Virtual Storage

Virtual Network

Virtualisation Layer

Vl-Ha

Hardware resources

Computing Hardware

Storage Hardware

Network Hardware

Nf-Vi

Virtualised Infrastructure Manager(s)

Execution reference points

Other reference points

Main NFV reference points

Proposed Next State, Proposed Policy change, Requested "state" info

Current "State" info

Current VNF info

Current VIM info

Current NFVI info

DARE

ENI

- For MANO to take full advantage of ENI, existing interfaces extension or in some cases, new interfaces may be required
- Physical Network interaction, e.g. with SDN Controller explicitly depicted through NFVI interaction (OOB possible too)

PoC Public demonstration plan

- ICISSP-2019 (23-25 Feb 2019)
  - As part of the workshop
    - NFV (Network Function Virtualization) as a foundation for security-as-a-service
  - Demo for ENI PoC – based on SHIELD
    - There will be available a Booth.

ICISSP 2019
5th International Conference on Information Systems Security and Privacy
Prague - Czech Republic | 23 - 25 February, 2019
INFORMATION
SECURITY
PRIVACY
TRUST

Thank you

SHIELD has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 700199