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

Project SHIELD: Securing against intruders and other threats through an NFV-enabled environment

InfoCom World 2018, Athens
21st November 2018

Olga E. Segou, PhD
Orion Innovations PC
osegou@orioninnovations.gr

SHIELD key facts and figures

European R&D project

Co-funded by the EU under H2020 "Secure Societies" programme

12 partners, 4.56 M€ total budget

Duration: Sep 2016 – Feb 2019 (30 months)

Internal release of the SHIELD system (alpha version):
September 2017

Open-source release of the SHIELD system (beta version):
September 2018

System tested & validated – Final open-source release:
February 2019

Motivation

During the past years, society has witnessed cyber-attacks being deployed with increasing frequency and impact, reaching even a global scale.

The need for cybersecurity investments is rising, and so do the costs.

Many experts, however, warn against the "security theatre", which is described as the case where organisations misplace their cybersecurity investments, leading to an inaccurate perception of improved security [2].

Organisations thus take up additional costs with little to no reduction in the overall risk.

Making arbitrary decisions without adequate threat intelligence can lead organisations to a patchwork of "stop-gap" solutions, deployed when a security need arises.

The SHIELD concept

SHIELD delivers an open solution for securing ISP and corporate networks with three tiers of protection:

- Cybersecurity services offer protection on the network level and detect attacks with known signatures (e.g. Firewall, Deep Packet Inspection, Intrusion Detection etc.)
- Big Data Analytics & Machine learning offer protection against attacks with unknown signatures and o-day vulnerabilities.
- Infrastructure Integrity Monitoring offers protection against malicious configurations and installed malware.

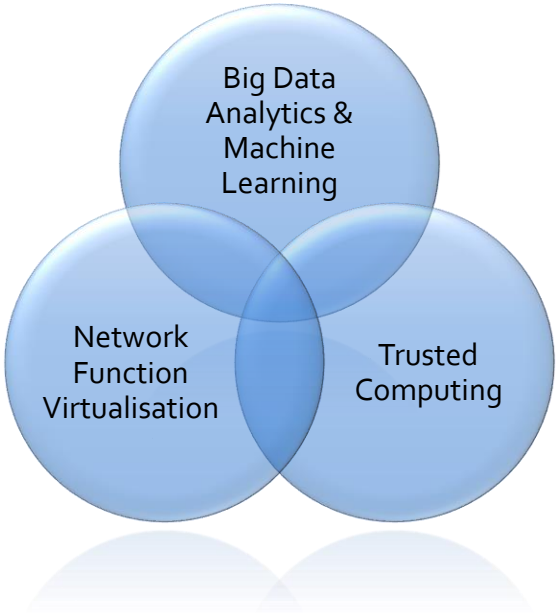
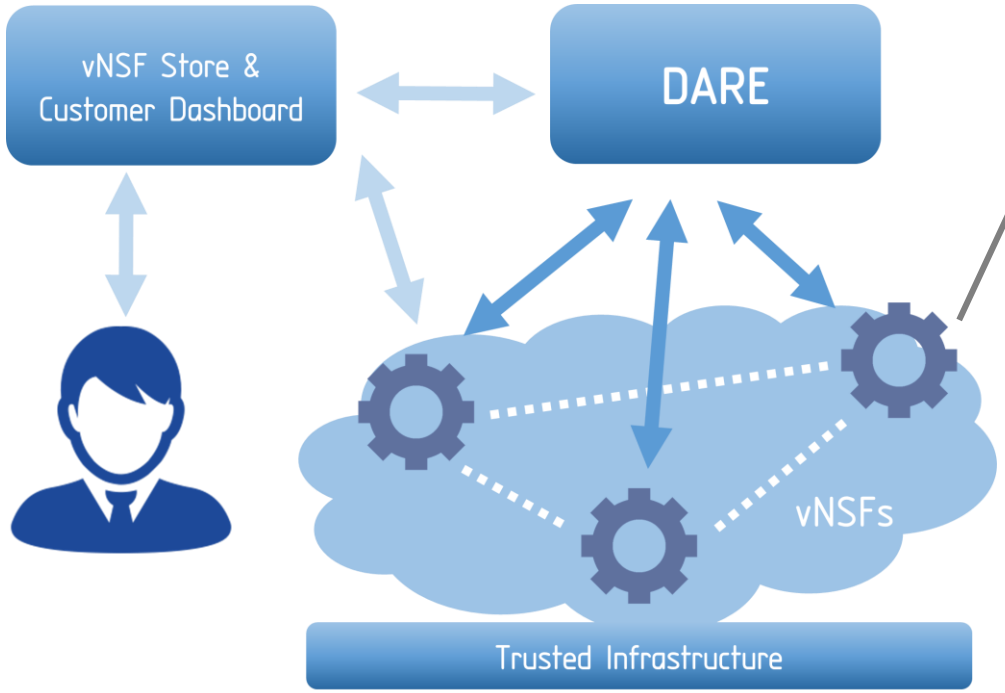


Figure 1: Main SHIELD concept.

The SHIELD system components (I)



VIRTUAL NETWORK SECURITY FUNCTIONS (VNSFS)

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

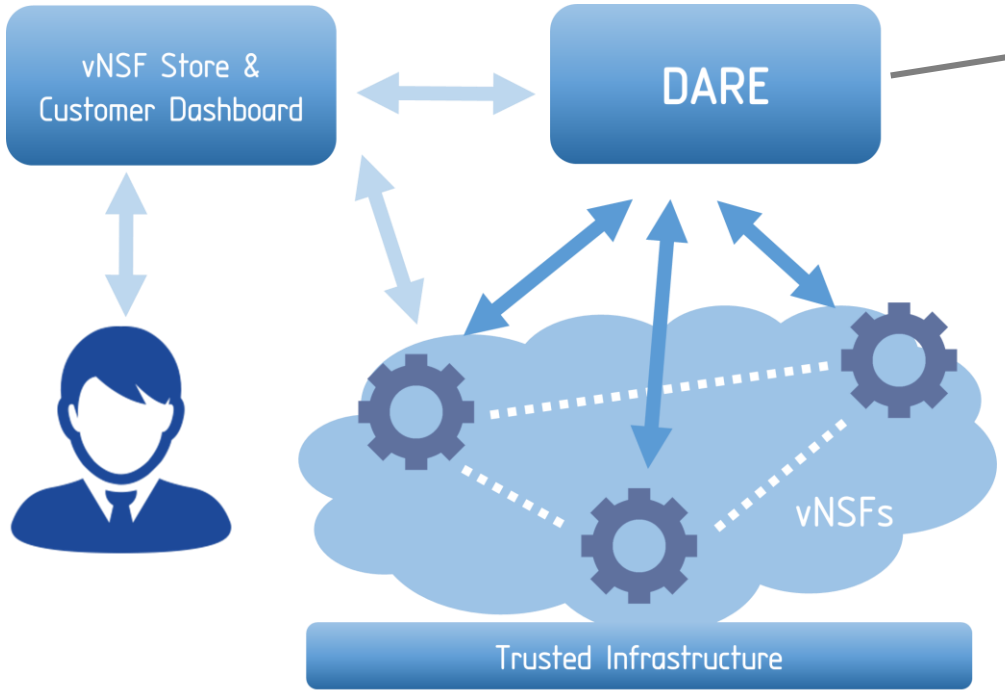
vNSFs are instantiated within the network infrastructure by a vNSF orchestrator in order to effectively monitor and filter network traffic in a distributed manner.

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

KEY TECHNOLOGIES

openstack. OPEN DAYLIGHT Open Source MANO TNOVA sonata

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.

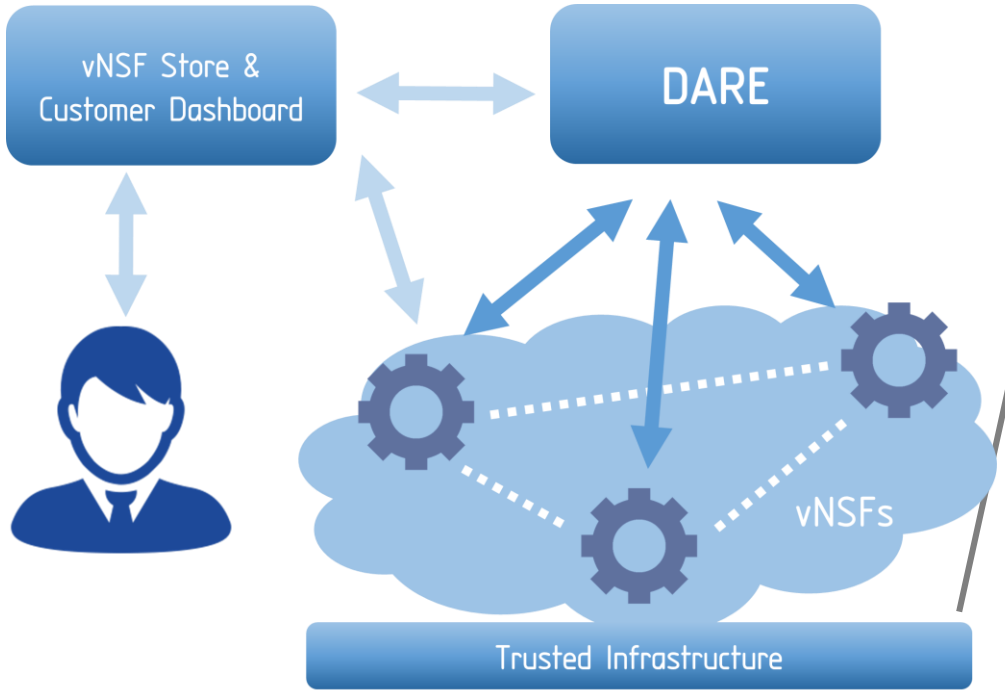
KEY TECHNOLOGIES

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

Positioning in the EMEA Cybersecurity market

- Per delivery mode, in EMEA region [3][4][5]:
  - **Standalone Products** [the main mode of delivery, with the largest market share]
  - **Managed Security Services** [high growth of 8,8% CAGR, expected to reach the market share of standalone products by 2020]
  - **Threat Intelligence** [highest growth rate of 14% CAGR]
  - **Security Orchestration Automation and Response (SOAR)** [nascent market for complete solutions featuring integrated workflows]
- Incident Response is the fastest growing category with Risk Assessment and Threat Intelligence and Mitigation closely following. Specifically, the 2016-2020 CAGR for "Incident Response and Forensics" is estimated at 14.9% while "Risk Assessment and Threat Intelligence" follow with 13.7%.
- **SHIELD can deliver relevant products in a fast-growing cybersecurity market, while positioning itself strategically in the nascent market for complete Security Orchestration Automation and Response (SOAR) solutions.**

SHIELD use cases

- **Use Case 1:** An ISP using SHIELD to secure their own infrastructure (Core & Edge)
- **Use Case 2:** An ISP is leveraging SHIELD to provide advanced SecaaS services to enterprise customers (horizontal or tailor made for specific verticals)
- **Use Case 3:** Contributing to national, European and global security.

- **SHIELD has successfully demonstrated protection against:**
  - Worm attacks (WannaCry detection and blocking with unsupervised neural networks in ~1min, with no prior knowledge or configuration)
  - Denial of Service (Distributed rate-based attacks, or protocol-based Slowloris, effectively detected and blocked)
  - Malicious web scripts (e.g. detection and blocking of Cryptojacking scripts)
  - Unwarranted cryptomining (Stratum protocol detection)
  - Data exfiltration detection (DNS tunneling, detection of malicious insider)

Watch our latest demos!

EU SHIELD PROJECT

- **Project overview**: https://www.youtube.com/watch?v=z8b-TQi2fvs
- **Year One demonstrations:**
  - 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
  - Detection of data exfiltration (DNS tunneling): https://www.youtube.com/watch?v=YxWxaIJW3ho
- **Year Two demonstrations:**
  - Detection of WannaCry: https://www.youtube.com/watch?v=7pZ7MH7PJ8M
  - Network Attestation: https://www.youtube.com/watch?v=3BNiR7es1f0
  - Detecting protocol-based Slowloris (slow DoS): https://www.youtube.com/watch?v=JwkzF0Vttbc
  - Cryptojacking blocking & Cryptocurrency mining detection: https://www.youtube.com/watch?v=mZIsvW_c98I

Follow us!

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

@shield_h2020

SHIELD EU Project

info@shield-h2020.eu

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

References

1. Ponemon Institute LLC and Accenture, “Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference,” https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017
2. Bruce Schneier, “Beyond Fear: Thinking Sensibly About Security in an Uncertain World (2n edition),” Copernicus Books, 2006.
3. https://news.ihsmarkit.com/press-release/technology/new-regulations-impact-emea-cybersecurity-market-2016-ihs-says
4. Ovum’s “Defining the next-gen managed security services provider” (Aug. 2017)
5. Anton Chuvakin, Augusto Barros, “Preparing your security operations for Orchestration and Automation tools”, Gartner, February 2018.