ENI ISG PoC Report
Securing against Intruders and Other Threats through a NFV-Enabled Environment (SHIELD)

1 General

Submission of this ENI ISG PoC Report as a contribution to the ENI ISG does not imply any endorsement by the ENI ISG of the contents of this report, or of any aspect of the PoC activity to which it refers.

2 ENI ISG PoC Report

2.1 PoC Project Completion Status

- Overall PoC Project Completion Status: completed

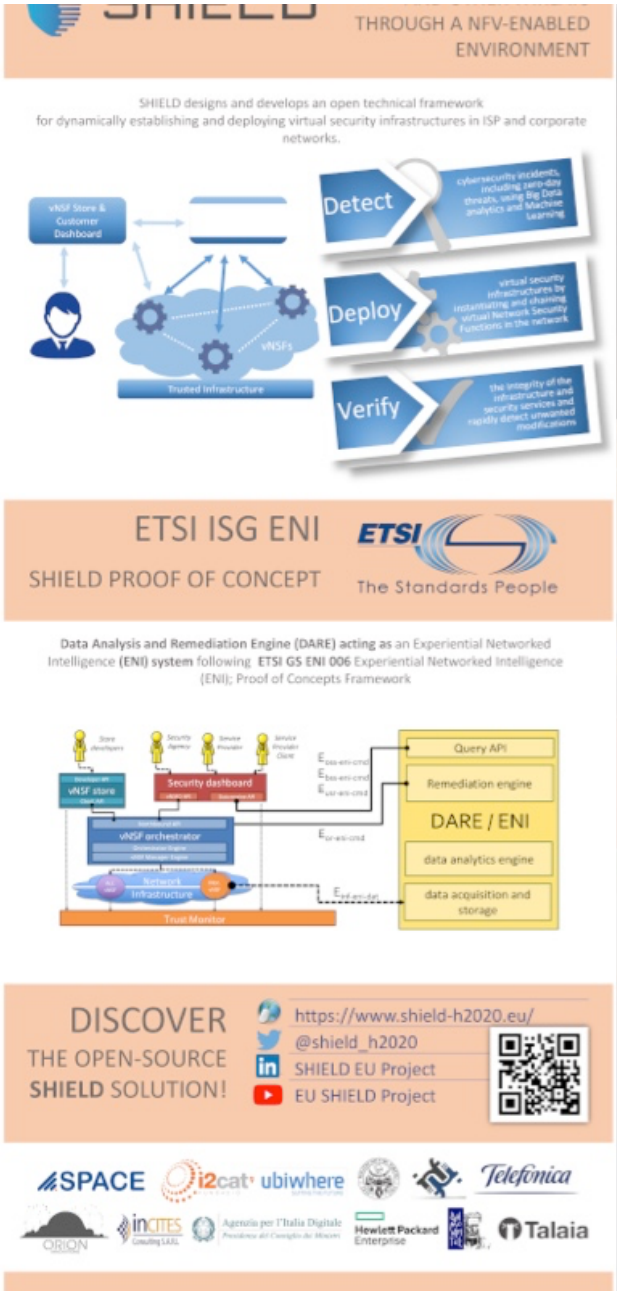
2.2 ENI PoC Project Participants

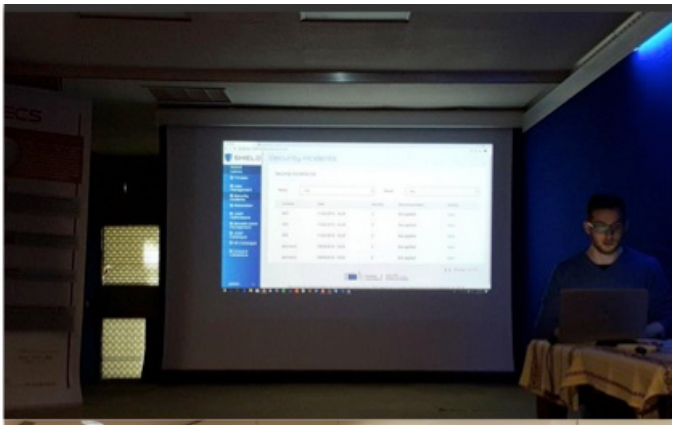
- PoC Project Name: Securing against Intruders and Other Threats through a NFV-Enabled Environment (SHIELD)
- Network Operator/Service Provider: Telefonica
  Contact: Antonio Pastor (antonio.pastorperales@telefonica.com)
- Manufacturer A: Space Hellas
  Contact: Georgios Gardikis (ggar@space.gr)
- Manufacturer B: ORION
  Contact: Olga Segou (osegou@orioninnovations.gr)
- Additional Members: Demokritos (NCSR)
  Contact: Eleni Trouva (trouva@iit.demokritos.gr)

2.3 Confirmation of PoC Event Occurrence

ICISSP 2019, Praga, Czech Republic, 23-25 February, 2019, http://www.icissp.org/Tutorials.aspx?y=2019

The PoC was presented during the tutorial session called “Modern Network-based Security: Softwarized Networking, Trusted Computing, and Artificial Intelligence for Cybersecurity” and during the full event at a dedicated booth.





2.4 PoC Goals Status Report

- PoC Project Goal #1: Demonstrate through a practical implementation how an AI framework can detect network attacks over an NFV network, with different Machine Learning algorithms and their combination.

  The goal has been fully demonstrated. The demonstration includes several ENI system interfaces and functional blocks interacting to solve a specific ransomware traffic attack (*Wannacry*) in an NFV environment. The DARE data analysis component providing the Cognition Management Functional Block was able to detect the specific network flows associated to the malware, using two different algorithm families sequentially executed (unsupervised anomaly detection and supervised classification).

- PoC Project Goal #2: Demonstrate a practical framework of a policy-driven control loop, by combining AI-based attack detection and proposing mitigation through an intent-based security policy to the network operator. This is accomplished by applying it through the translation into a specific configuration of VNFs.

  The goal has been fully demonstrated. The demonstrator showed how an additional DARE component (the remediation engine), using as an input the results provided by the ML algorithms, could provide a set of specific recommendations to mitigate the attack and send it to the Assiste system represented through the SHIELD

network operator dashboard. This latter component combines several functional blocks: the Context-Aware Management Functional Block, the Policy Management Functional Block and the Denormalization and Output Generation.

- PoC Project Goal #3: Demonstrate how the use of remote attestation[1] technology (i.e. a method by which a host -client- authenticates its hardware and software configuration to another remote host -server-) allows to avoid device and data collecting corruption and tampering.

  The goal has been fully demonstrated. The SHIELD component called Trust Monitor was able to demonstrate how, after deploying a dockerized network function (a dummy VNF that simulated a telemetry generation device) with an OSM orchestrator, it was able to detect a manipulation in the integrity of the VNF (an alteration of the content of the filesystem).

2.5 PoC Feedback Received from Third Parties (Optional)

The ICISSP PoC was focused on security, with high emphasis on the AI applicability in this area. Most relevant comments that could apply to ENI are:

- **The ENI system should be open and scalable**. Some experts in AI/ML suggested to provide interfaces or reference points for the interaction between different ENIs, enabling knowledge sharing. As an example, the interaction of AI cloud services with an internal ENI system was specifically mentioned.

- **AI performance** is one the main topics discussed around AI models (AuC, precision, recall, accuracy, etc.). The capacity to define and benchmark the performance of the used AI models was mentioned. Including this measurement capacity in the framework would allow to compare different models, and therefore decide on adding or removing them from the ENI System.

3 ENI PoC Technical Report (Optional)

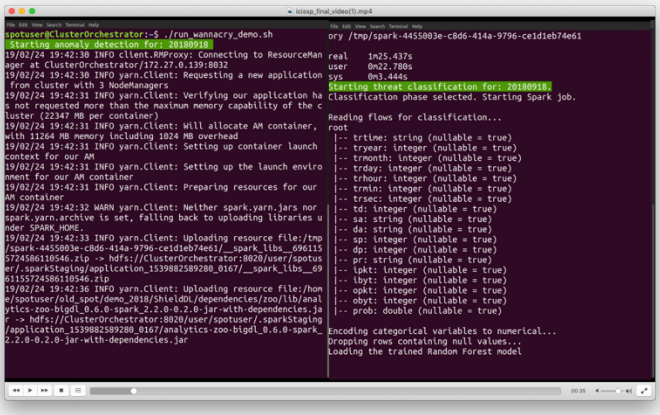
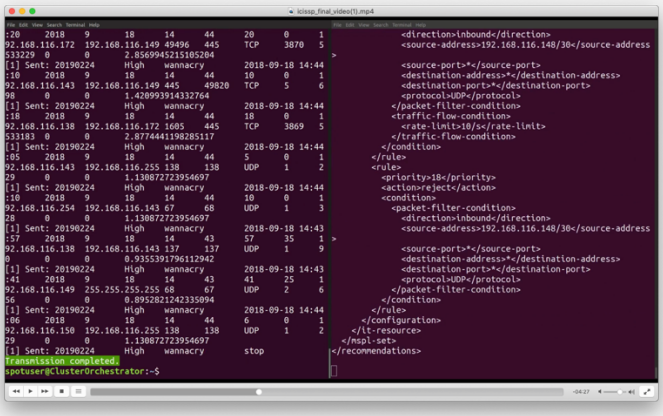
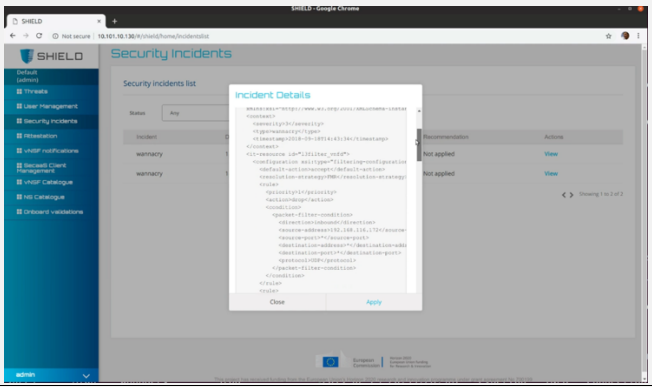
3.1 General

The PoC was organized over two different scenarios

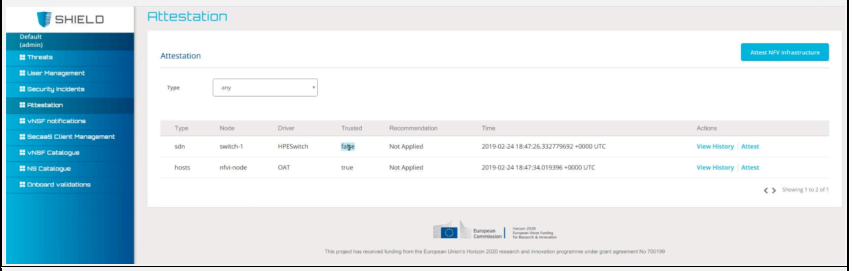
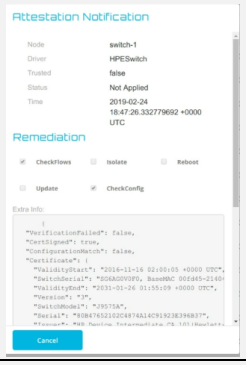
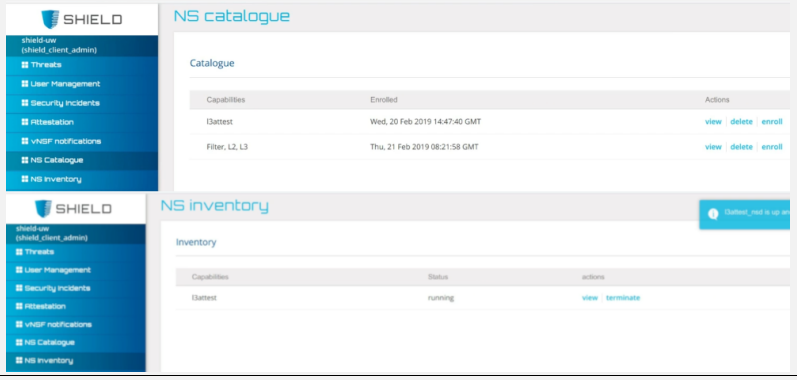
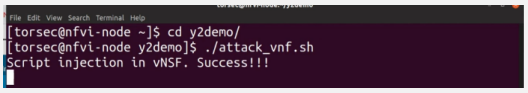
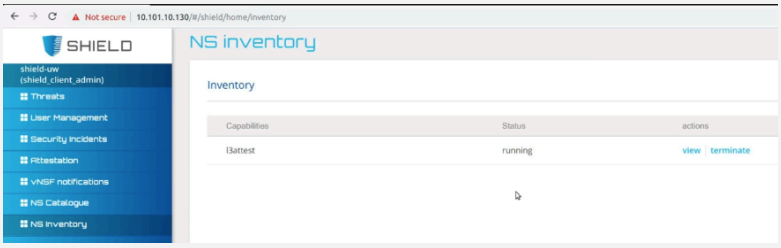
1. Ransomware attack (PoC goal #1 and #2)
2. Integrity verification (PoC goal #3)

[1] ETSI GR NFV-SEC 007 and https://www.ietf.org/id/draft-pastor-i2nsf-nsf-remote-attestation-06.txt

Scenario 1: Ransomware Attack

Scenario:	Ransomware attack
Motivation:	Detect and mitigate as soon as possible a nearly 0-day attack using ransomware (i.e. a malware that kidnaps / encrypts files and asks for a ransom)
Sequence:	
1. The traffic of a network infection with Wannacry is replicated (original data collected on 18th Sept. 2018)	
2. Traffic is collected from the network in netflow format by the DARE.	
3. The data is stored and normalized (dataset extraction and feature selection)	
4. An unsupervised learning model (deep learning autoencoder algorithm) process and detect a set of anomalous flows in the stored data 5. A supervised model (Random Forest classification algorithm) identifies the Wannacry attack and provides the affected network flows	
6. These data progress to the remediation engine that, based on the classification identification, chooses a "ransomware recipe" (policy template) that maps an intent-based security policy (HSPL) onto an associated detailed policy with higher granularity(MSPL)	
7. The MSPL is sent to the Dashboard as a recommendation of action to be applied	
Results:	The Operator eventually accepts the recommendation and applies the policy that filters all traffic from the infected IPs

Scenario 2: Integrity Verification

Scenario:	Integrity verification
Motivation:	Ensure the integrity of the network infrastructure (physical or virtualized) involved in the data generation for the ENI system(s). The objective is to avoid any deliberate manipulation of the ENI system through the data collected from network SDN switches, physical servers and VNFs.
Sequence:	
1. The NFVI infrastructure (switches, hosts and VNFs) is periodically attested by the service provider	
2. The SDN switch goes in an untrusted state by the manipulation of the firmware or the local forwarding database. The switch is restored to initial state and remediation is shown in the dashboard	
3. Service provider accesses the dashboard, enrols a new VNFs and instantiates it.	
4. Periodic attestation is used to confirm trusted state.	
5. The VNF is manipulated by injecting code, so its integrity is compromised	
6. Next periodic attestation detect the manipulation and reports an untrusted state.	
Results:	The client terminates the VNF and eventually redeploys a clean one that will guarantee data generation is not altered

3.2 PoC Contribution to ENI ISG

Table 1

Contribution	WG/EG	Work Item (WI)	Comments
New security use case		ETSI GR ENI 001	*Propose a new category "Security" and added Use case #5-2*

3.3 Gaps identified in ENI standardization

Table 2

Gap Identified	Forum (ENI ISG, Other)	Affected WG/EG	WI/Document Ref	Gap details and Status
Inference model interactions	ENI		ETSI GS ENI 005	Inference model families can be combined to improve the cognition framework. The PoC was able to use different inference models and apply knowledge transfer between them. It would be desirable to ad a reference point and the capacity to add third party inference models or other ENI systems
Data collection integrity and security	ENI		ETSI GS ENI 005	Data integrity and data security in the Data Collection and Analysis FB is needed. The PoC demonstrated a trust monitoring functional block to detect tampering within the infrastructure, including VNFs to guarantee that AI is not manipulated.
intent-based policies in the closed loop	ENI		ETSI GS ENI 005	The PoC required the Policy Management to work with intent policies (human language for operators: HSPL) and their translation to imperative policies (understandable by assisted system: MSPL). The translation must be synchronized and automatized to avoid errors

3.4 PoC Suggested Action Items

None.

3.5 Additional messages to ENI

None in addition to the matters discussed above.

3.6 Additional messages to Network Operators and Service Providers?

None.