SHIELD

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

[H2020 - Grant Agreement No. 700199]

Application of distributed computing & machine-learning technologies to cybersecurity

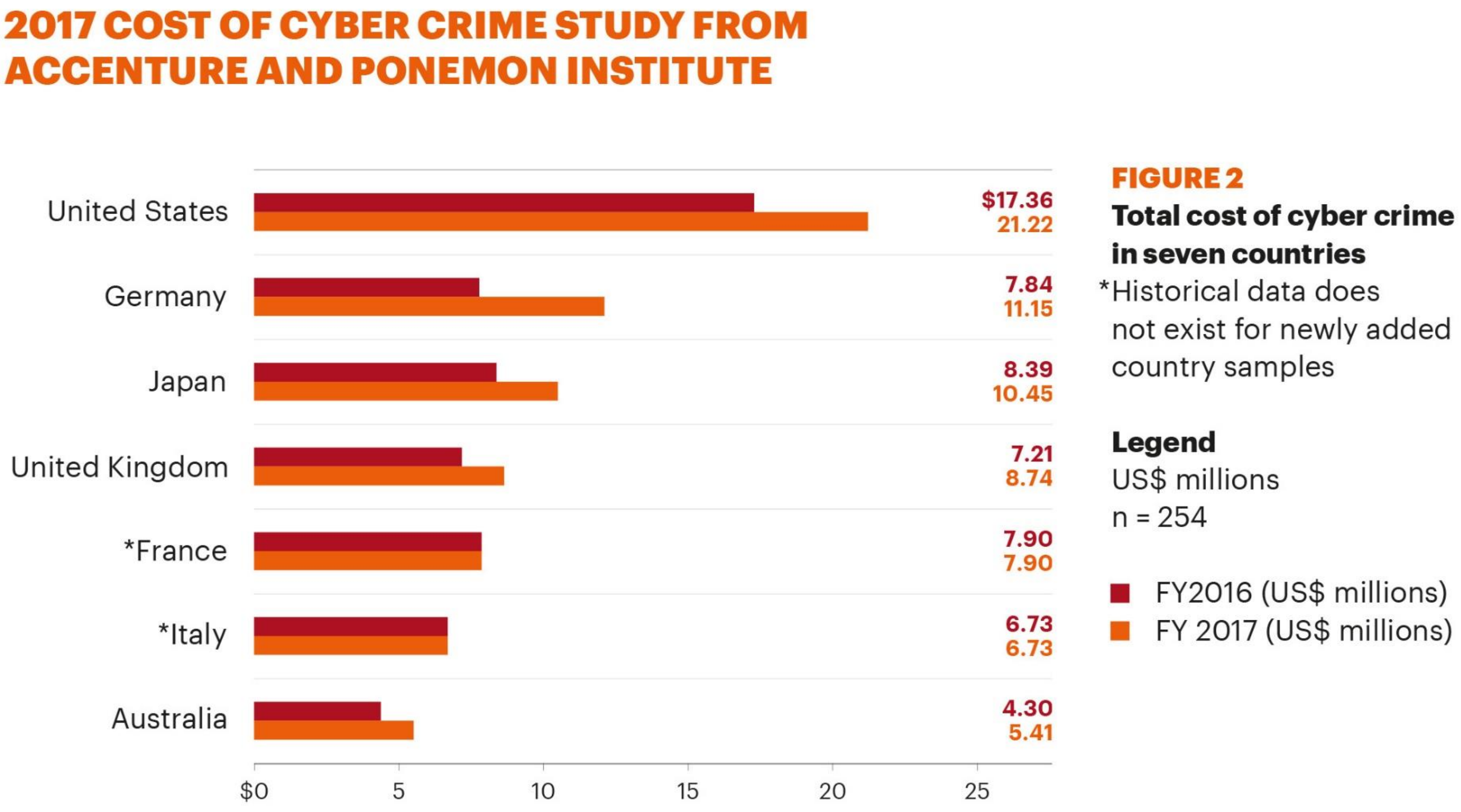
Hamza Attak, Marc Combalia, Georgios Gardikis, Bernat Gastón, Ludovic Jacquin, Dimitris Katsianis, Antonis Litke, Nikolaos Papadakis, Dimitris Papadopoulos, Antonio Pastor, Marc Roig, Olga Segou

Presenter:
Dimitris Papadopoulos
Infili Technologies P.C.

C&ESAR 2018
Artificial Intelligence
& Cybersecurity

SPACE i2cat ubiwhere POLITECNICO DI TORINO Telefonica ORION INNOVATIONS inCITES Consulting S.A.R.L Agenzia per l'Italia Digitale Presidenza del Consiglio dei Ministri Hewlett Packard Enterprise Talaia

The motivation



Source: Accenture and Ponemon, "2017 Cost of Cyber Crime Study"

The motivation

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

Huge momentum of open technologies for Big Data analytics

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

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

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)

Our team

SPACE

i2cat FUNDACIÓ

Hewlett Packard Enterprise

inCITES Consulting S.A.R.L

infili

ΔΗΜΟΚΡΙΤΟΣ

ORION INNOVATIONS

POLITECNICO DI TORINO 1859 1906

Telefónica

Telefónica I+D

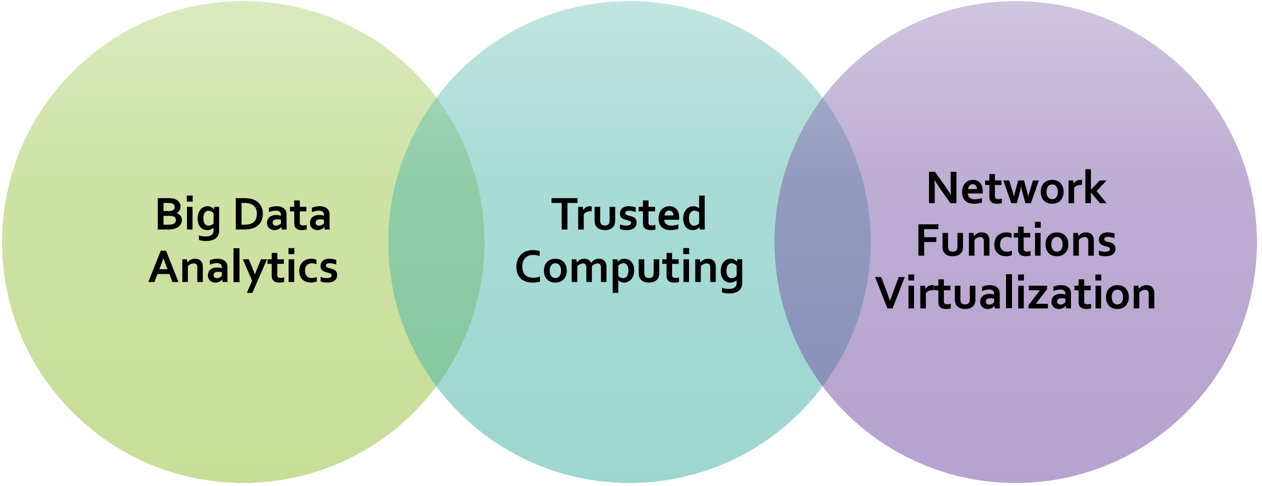
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Talaia NETWORKS

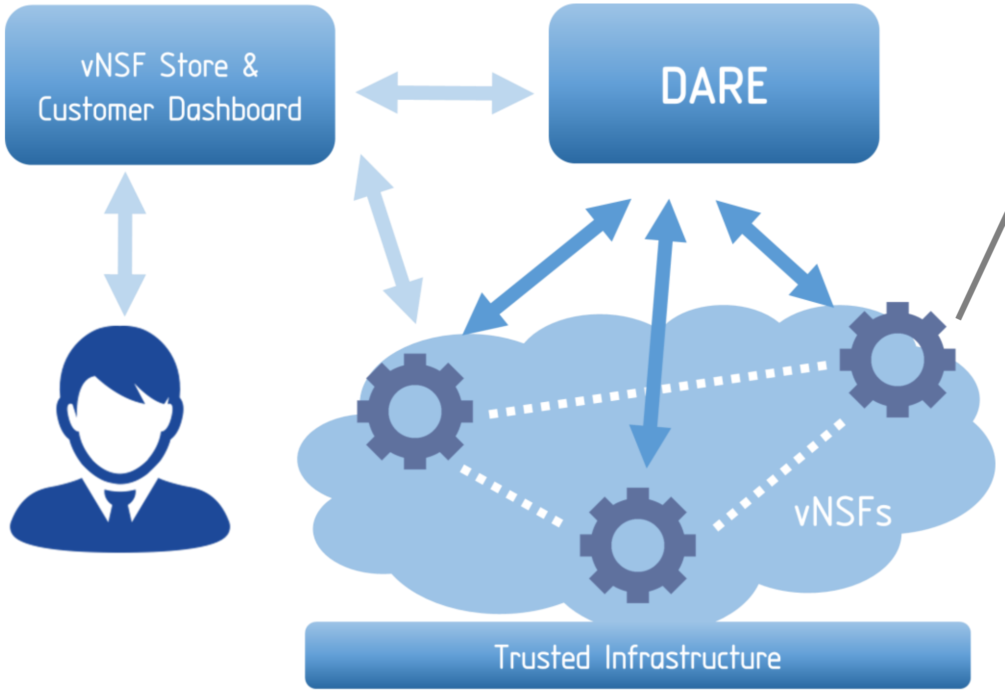
ubiwhere

Project mission

SHIELD is a distributed cyber-security system that aims to deliver an open solution for dynamically establishing and deploying virtual security infrastructures in ISP and corporate networks.



The SHIELD system components (I)



KEY TECHNOLOGIES

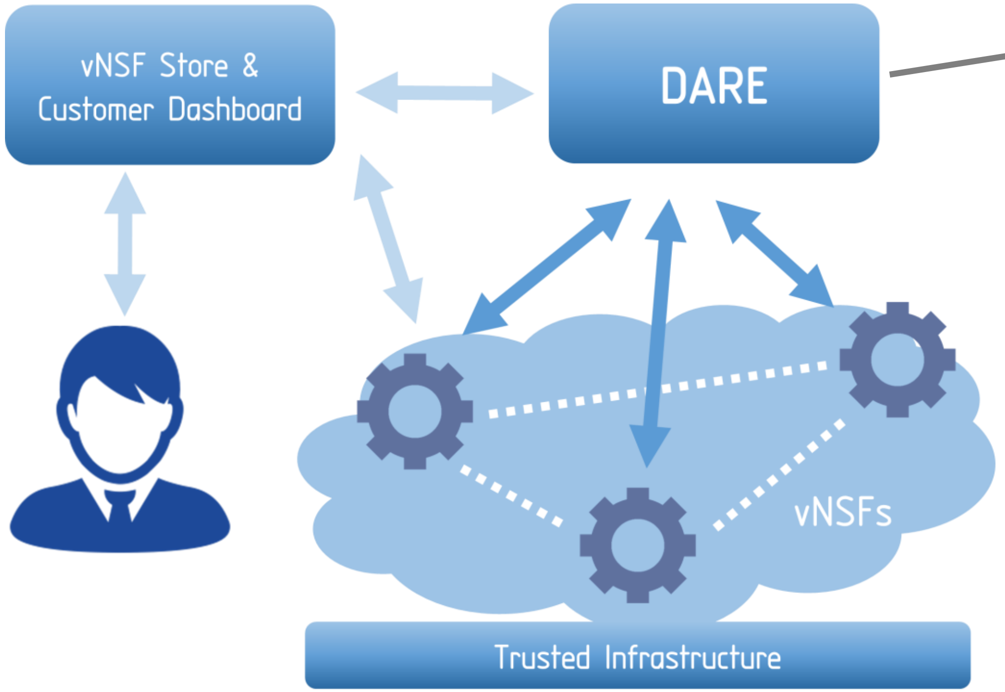
openstack · OPEN DAYLIGHT · Open Source MANO · TNOVA · sonata

VIRTUAL NETWORK SECURITY FUNCTIONS (VNSFS)

Security as-a-Service (SecaaS) based on virtualized 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.

The SHIELD system components (II)



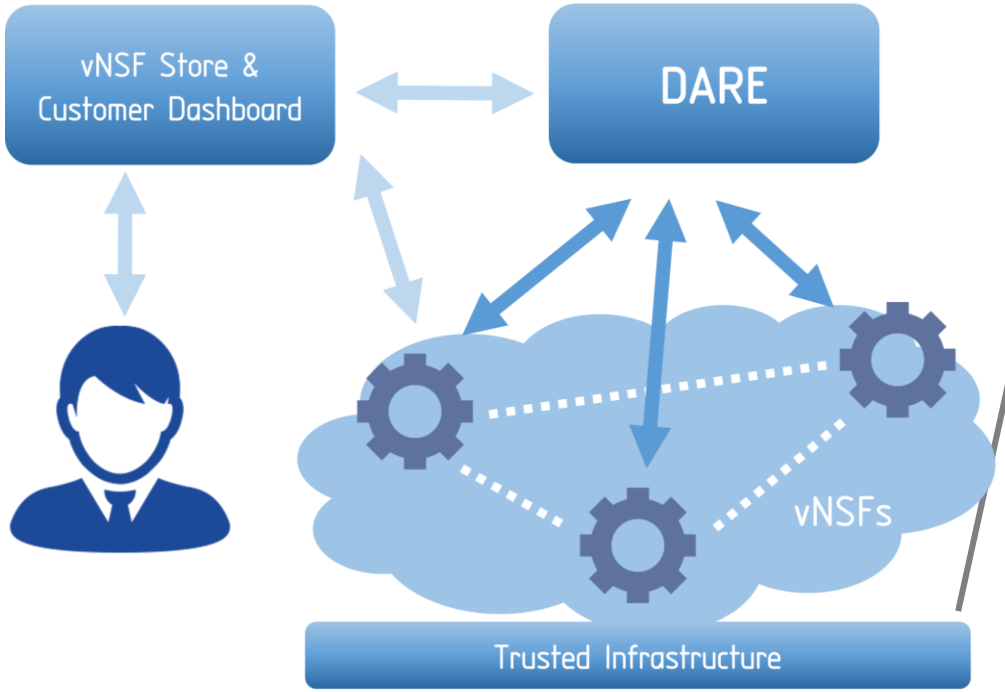
KEY TECHNOLOGIES

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.

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

The SHIELD system components (III)



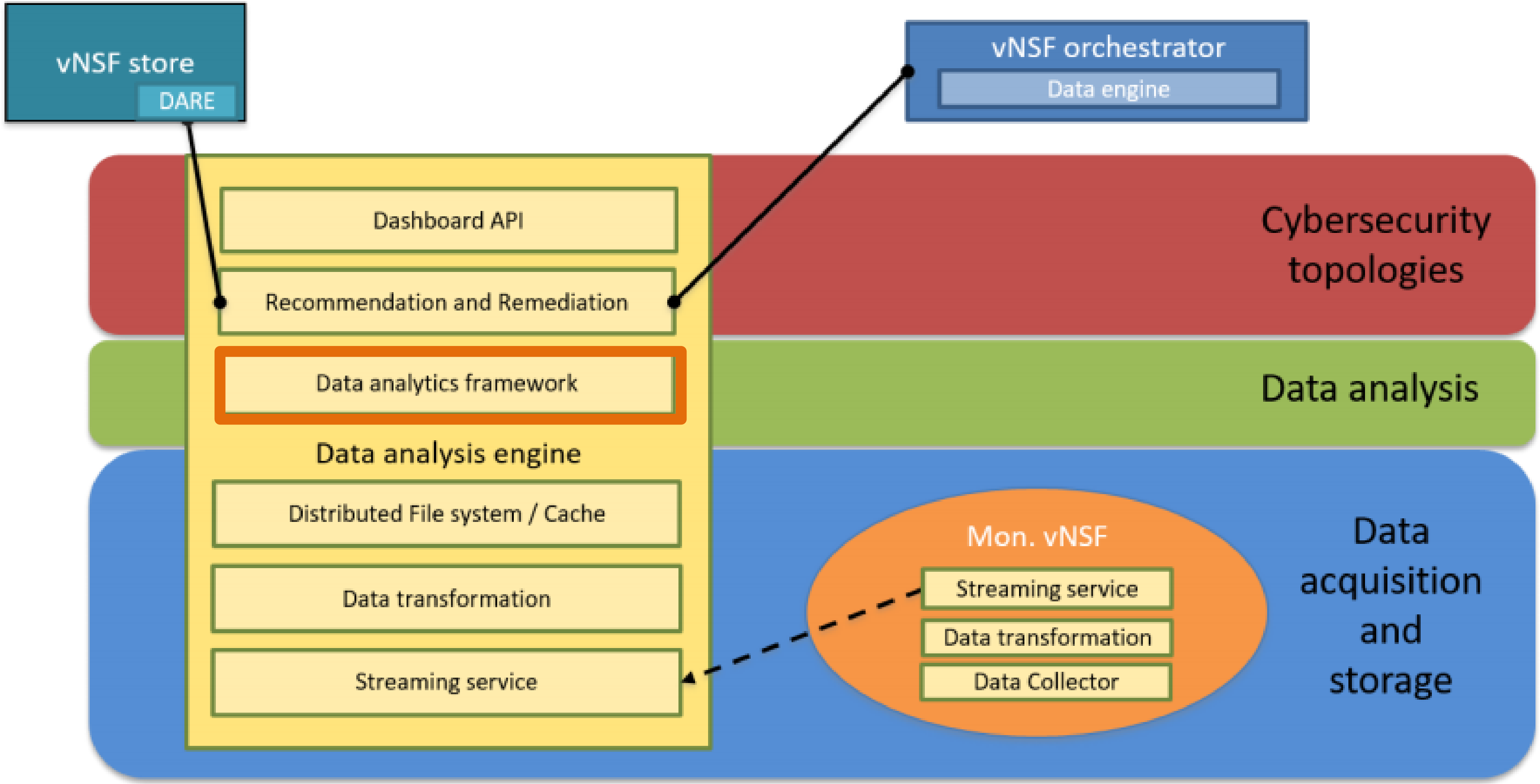
KEY TECHNOLOGIES

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).

DARE: the heart of SHIELD analytics

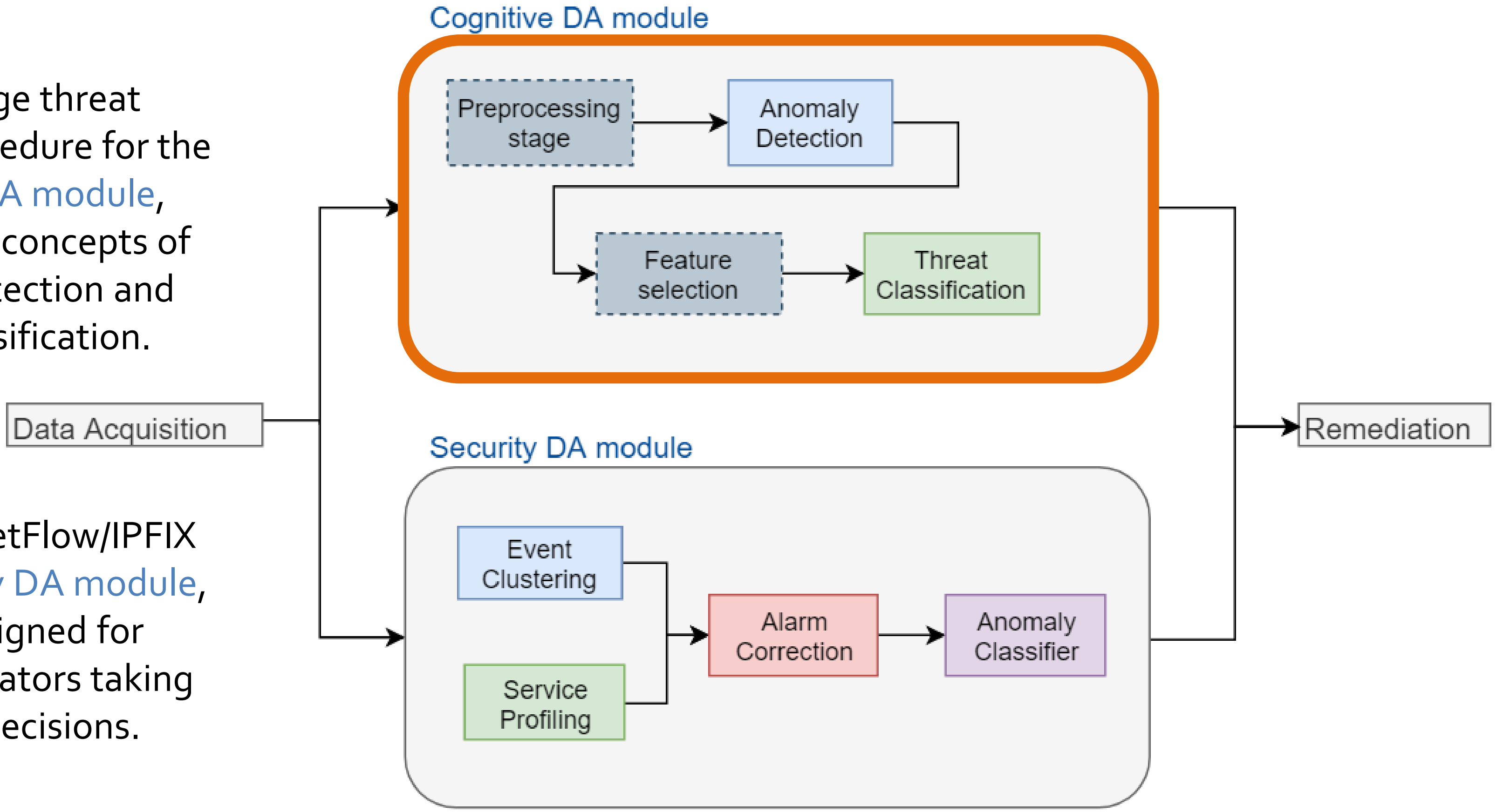


Modular analytics

Focusing on open-source, scalable **machine-learning & deep-learning** models for cybersecurity.

A two-stage threat detection procedure for the Cognitive DA module, based on the concepts of anomaly detection and threat classification.

A scalable, NetFlow/IPFIX based Security DA module, that is designed for network operators taking complex decisions.



The Cognitive DA module

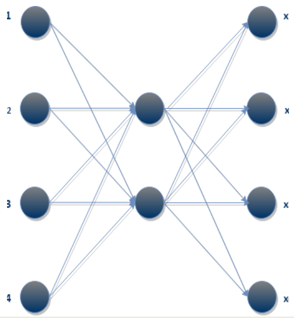
Based on Apache Spot:

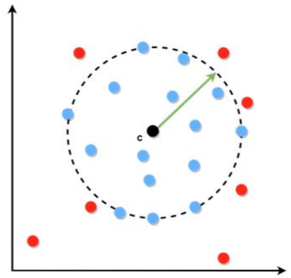
- Centralized ingestion
- Single threat ingestion
- Single "Bag of words" algorithm for anomaly detection (Latent Dirichlet Allocation, *LDA*)
  -No real time
  -No evaluation possible
- No classification mechanism
- Spot dashboard

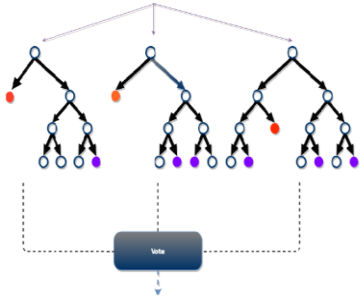
After SHIELD extensions:

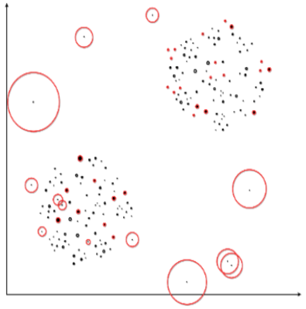
- Distributed ingestion using Spark Streaming
- Multi-threat ingestion
- **NRT Anomaly Detection:**
  -Autoencoder
  -One-Class SVM
  -Isolation Forest
  -Local Outlier Factor
- **NRT Classification:**
  -Random Forest
  -MultiLayer Perceptron
- SHIELD dashboard

Anomaly Detection models





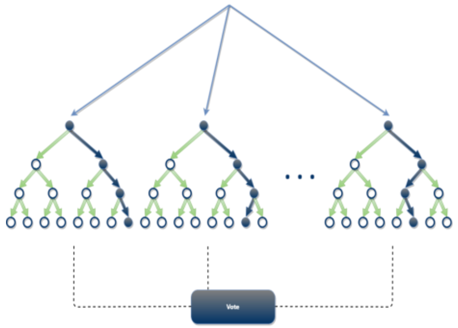




Autoencoder	One-class SVM	Isolation Forest	Local Outlier Factor
A type of ANN used to learn efficient data encodings in an unsupervised manner.	An unsupervised ML algorithm that learns a decision function for novelty detection.	A tree-based ensemble method, built on the basis of decision trees.	An unsupervised ML algorithm, based on outlier detection.
The most used architecture for anomaly detection.	It aims at estimating the support of a distribution by identifying regions where most of the cases lie.	Explicitly identifies anomalies instead of profiling normal data points	The concept of finding anomalous data points by measuring their local density with respect to their neighbors.
Relies on input signal rebuilding after putting it through a compressive path.	Non-linear decision boundaries using non-linear functions in hyper-planes through Kernel functions.	Partitions are created by randomly selecting a feature and a splitting value between its minimum and maximum.	Locality is given by k-nearest neighbors, whose distance is used to estimate the density.
After training, the autoencoder can optimally reconstruct data similar to the one it was trained with.	The points within the decision boundaries are considered normal cases.	On average, a normal point requires more partitions to be identified than an abnormal point.	Regions of similar density correspond to normal data points.
Anomalies will present a high reconstruction error rate after being forwarded through this architecture.	Points whose distance to the center is greater than the radius are considered anomalies.	Outliers are less frequent than regular observations and require less splits (closer to the root of the tree)	Points that have a substantially lower density than their neighbors can be considered to be outliers.

Threat Classification models

Random Forest



A tree-based ensemble supervised learning method used for classification

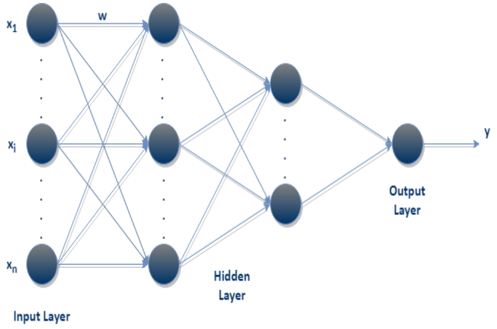
One of the best-performing classifiers, due to its lack of overfitting and its unmatched classification accuracy.

Constructs a multitude of decision trees at training and outputs the mode of the classes of the individual trees

Applies the bagging technique to tree learners, leading to better performance by decreasing the variance, without increasing the bias

Able to distinguish between the different threat classes as well as normal traffic.

MultiLayer Perceptron



A class of ANNs, consisting of at least three layers of nodes (input, hidden, and output layers).

Each neuron unit calculates the linear combination of its real-valued inputs and passes it through a threshold activation function.

Non-linear activation are implemented, allowing to solve non-linearly separable problems.

Learning occurs iteratively, by changing connection weights after each piece of data is processed, based on error backpropagation.

Able to classify multiple normal and anomalous states, after being trained for several epochs.

Realistic datasets for performance evaluation

Monday: Benign traffic only

Tuesday: Bruteforce attack using a variety of password cracking tools.

Wednesday: DoS attacks using a 4 different tools and Heartbleed attack.

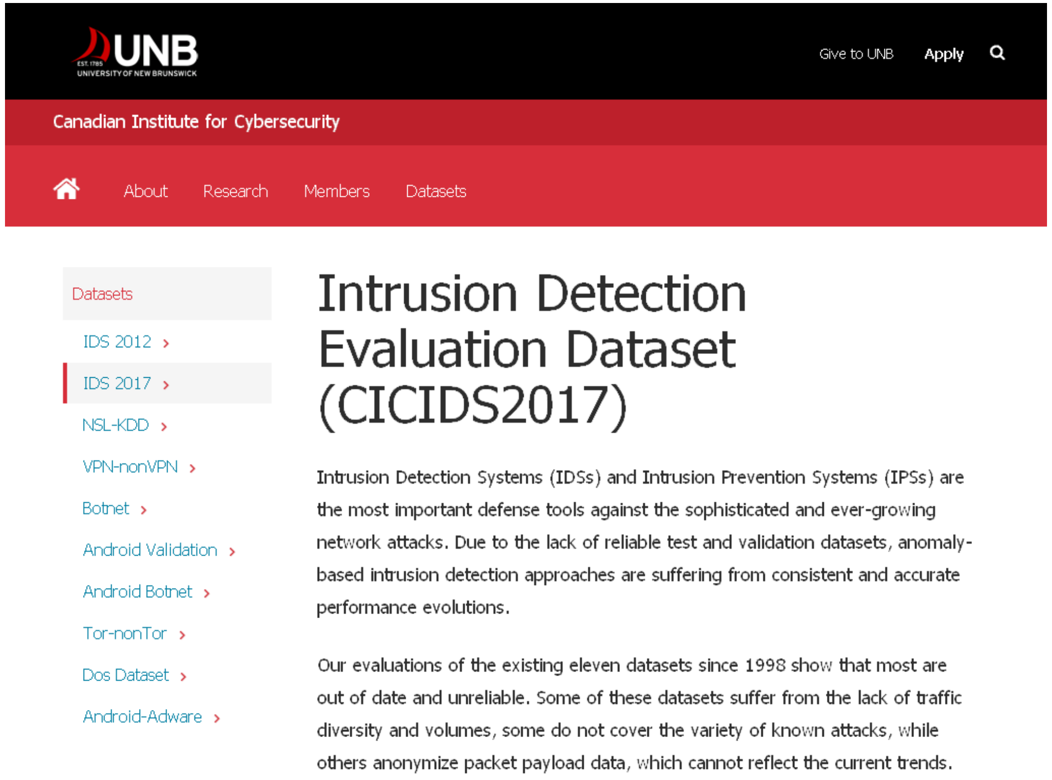
Thursday morning: Web attack using the Damn Vulnerable Web App (DVWA).

Thursday afternoon: Infiltration attack using Metasploit.

Friday morning: Botnet attack using ARES.

Friday Afternoon: DDoS attack using the Low Orbit Ion Canon (LOIC).

Friday Afternoon-2: Portscan attack over the all Windows machines.


UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK

Give to UNB Apply

Canadian Institute for Cybersecurity

About Research Members Datasets

Datasets
- IDS 2012 ›
- IDS 2017 ›
- NSL-KDD ›
- VPN-nonVPN ›
- Botnet ›
- Android Validation ›
- Android Botnet ›
- Tor-nonTor ›
- Dos Dataset ›
- Android-Adware ›

Intrusion Detection Evaluation Dataset (CICIDS2017)

Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are the most important defense tools against the sophisticated and ever-growing network attacks. Due to the lack of reliable test and validation datasets, anomaly-based intrusion detection approaches are suffering from consistent and accurate performance evolutions.

Our evaluations of the existing eleven datasets since 1998 show that most are out of date and unreliable. Some of these datasets suffer from the lack of traffic diversity and volumes, some do not cover the variety of known attacks, while others anonymize packet payload data, which cannot reflect the current trends.

Source: https://www.unb.ca/cic/datasets/ids-2017.html

The CICIDS2017 benchmark dataset contains the abstract behaviour of 25 users for 5 days (50,1GB of PCAPs)

Realistic datasets for performance evaluation

MALWARE-TRAFFIC-ANALYSIS.NET

2017-05-18 - GUEST BLOG BY DAVID SZILI - PCAP OF WANNACRY SPREADING USING ETERNALBLUE

EDITOR'S NOTE:

- This blog post was submitted by **David Szili**, an independent IT security consultant based in Luxembourg.
- David had emailed a pcap from his test environment with traffic showing WannaCry ransomware spreading using the EnternalBlue exploit.
- I thought this would make a good guest blog, so enjoy!

ASSOCIATED FILE:

- ZIP archive of the pcap: **2017-05-18-WannaCry-ransomware-using-EnternalBlue-exploit.pcap.zip** 23.9 MB (23,857,652 bytes)
- ZIP archive of the WannaCry ransomware sample: **24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe.zip**

TEST ENVIRONMENT

The following Windows servers and workstations were established in a LAN environment:

(Read: IPv4 address - MAC address - Host descritpion - Host name)

- 192.168.116.143 - a4:1f:72:20:54:01 - Windows 2012 R2 domain controller - TestDC1
- 192.168.116.150 - a4:1f:72:49:11:6d - Windows 2012 R2 server with a file share - WIN-2012-R2-1

- 192.168.116.138 - 00:19:bb:4f:4c:d8 - Windows 7 x64 - domain-joined workstation - DFIR_Win7_x64
- 192.168.116.149 - 00:25:b3:f5:fa:74 - Windows 7 x86 - domain-joined workstation - DFIR_Win7_x86
- 192.168.116.172 - 00:1c:c4:33:c6:dd - Windows 7 x86 - clone of DFIR_Win7_x86 - C-DFIR_Win7_x86

MALWARE

The following information covers the WannaCry ransomware sample used to generate this traffic:

- SHA256 hash: 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
  SHA1 hash: e889544aff85ffaf8b0d0da705105dee7c97fe26
  MD5 hash: db349b97c37d22f5ea1d1841e3c89eb4
  File size: 3.6 MB (3,723,264 bytes)
  File type: Win32 EXE

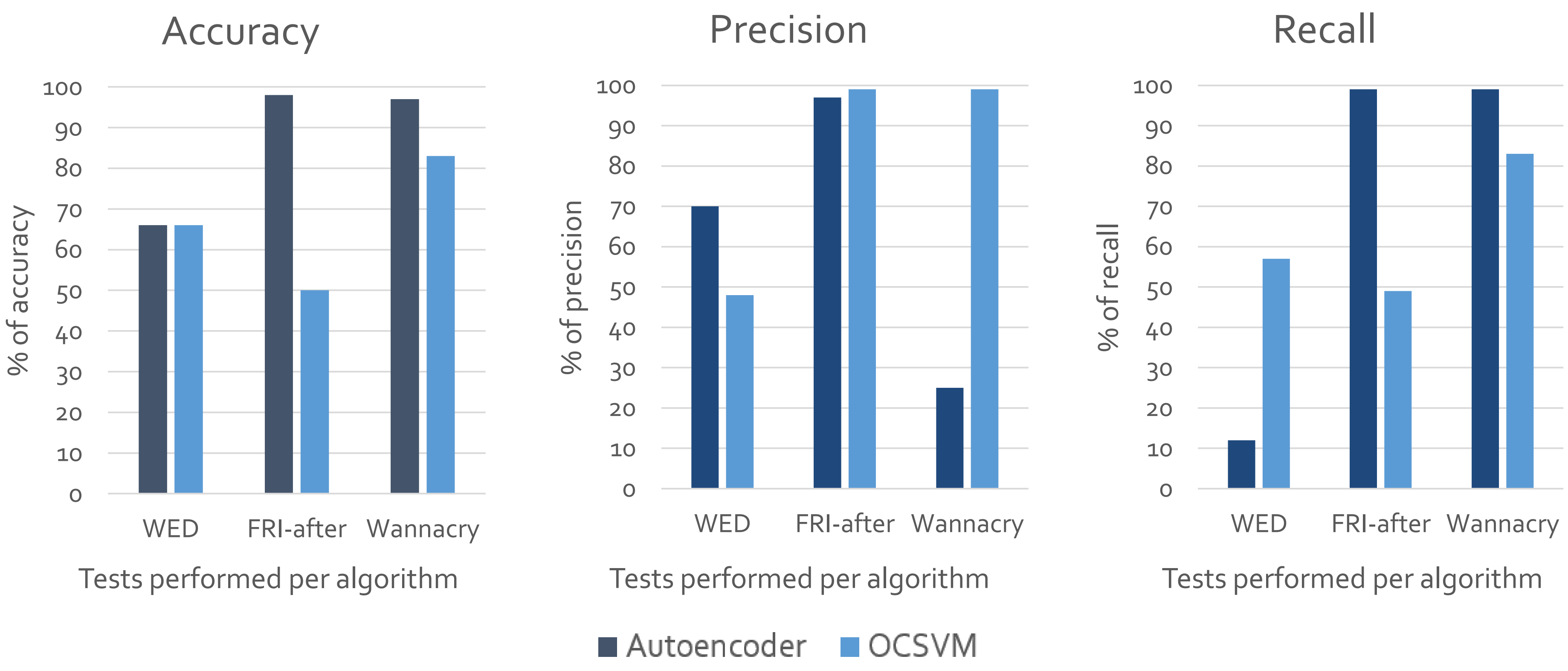
References for the above sample:

Source: https://www.malware-traffic-analysis.net/2017/05/18/index2.html

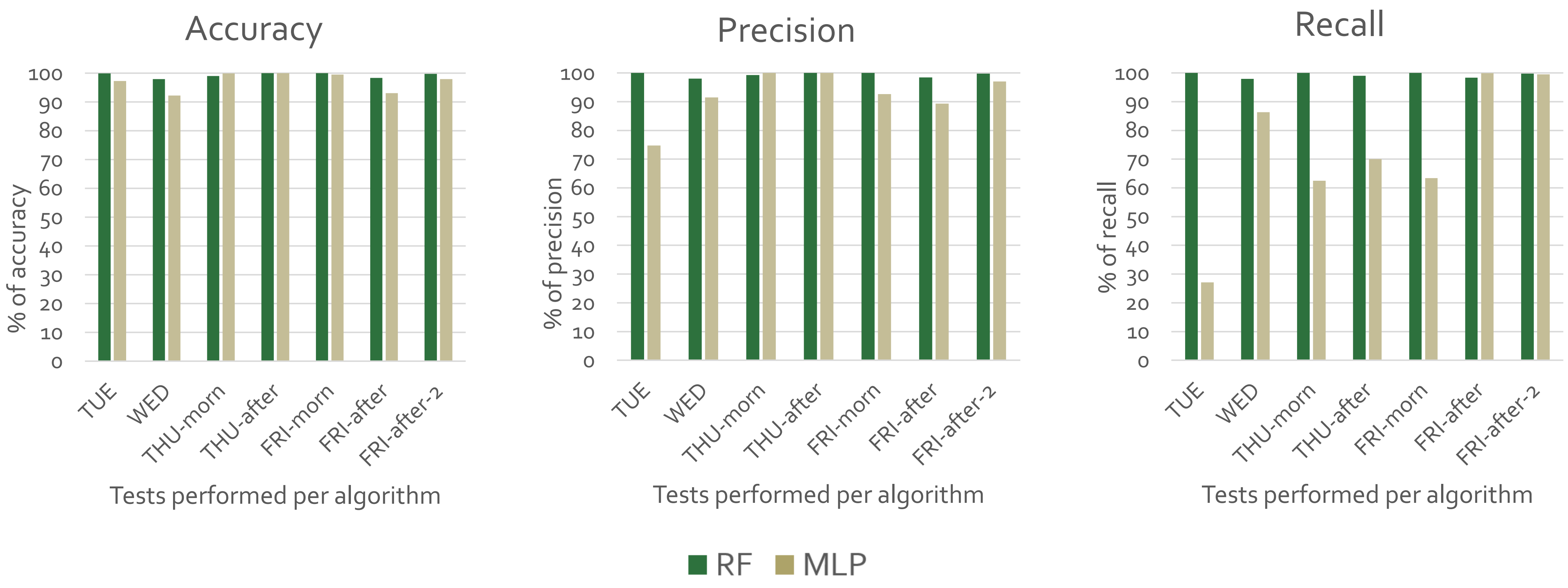
A sample of the WannaCry ransomware was also exploited, containing 23.9 MB of PCAPs.

The aim of our cybersecurity solution is to detect anomalies by leveraging the ***Netflow traffic protocol*** *(NFCAPD),thus only features that are present in this protocol were used in the analysis procedure.*

Anomaly detection results



Threat classification results



Conclusions and future work

Deep Learning **Autoencoders** seem to have a **very high potential** but as often, DL algorithms need to be finely tuned in order to obtain stable results and avoid performance issues

The tree-based **Random Forest** and the **MultiLayer Perceptron** models both obtained **remarkable results** that exceed the performance of other reported algorithms on the same dataset, with the former being more robust in multiclass classification problems.

For future work:

- Include more types of modern attacks in different OSI layers, as well as combine them with the existing ones for the evaluation of all our proposed models on a comprehensive dataset.
- Examine feature selection and resampling techniques to further improve our detection results.

Key project milestones

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

Current status

- ✓ (Updated) User requirements and high-level system architecture updated
  - Publicly available at: https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D2.2_Updated_requirements,_KPIs,_design_and_architecture_v.1.0.pdf
- ✓ Detailed architecture and technical specs of subsystems
  - Publicly available at: https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D3.2_Updated_specifications,_design_and_architecture_for_the_vNSF_ecosystem_v1.0.pdf
  - https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D4.2_Updated_specifications,_Design_and_Architecture_for_the_Usable_Information-Driven_Engine_v1.0.pdf

Check out our latest demos!

YouTube 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 the Cognitive DA module: https://www.youtube.com/watch?v=YxWxaIJW3ho
- Y2 Review demos (containing Slowloris DoS, Wannacry and cryptojacking detection) will soon be available.

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