ESORICS Workshop - CPS4CIP 2021 : The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection

SPHINX

A Universal Cyber Security
Toolkit for Health-Care Industry

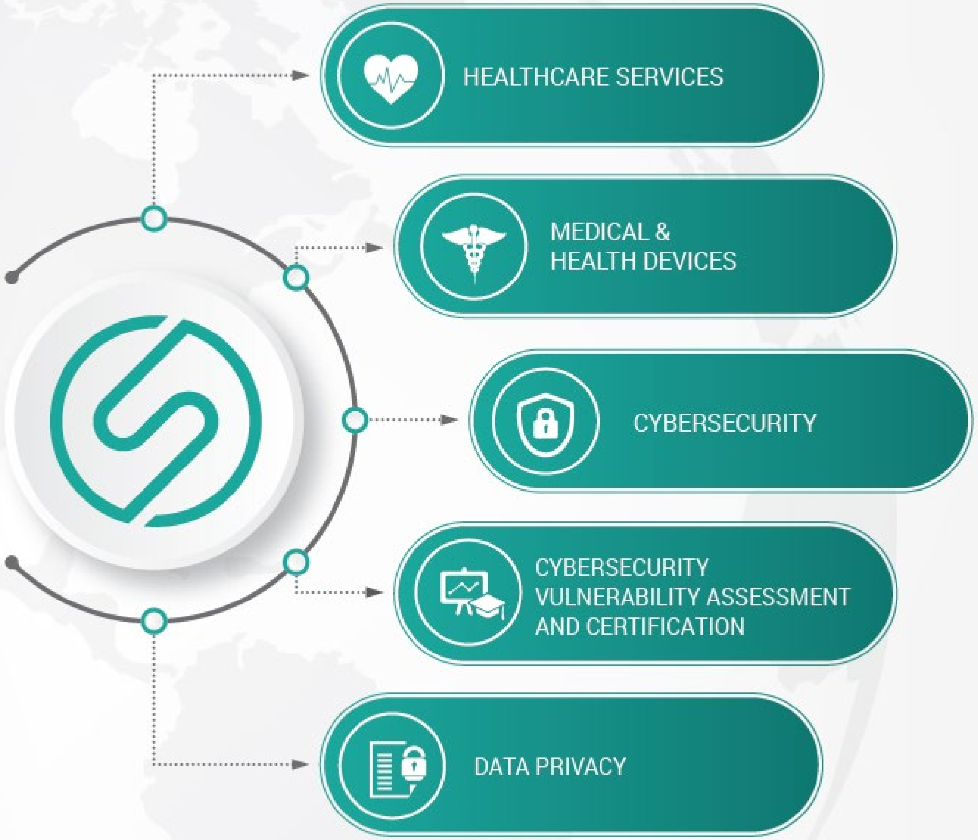
Sphinx - A Universal Cybersecurity Toolkit for Healthcare Sector

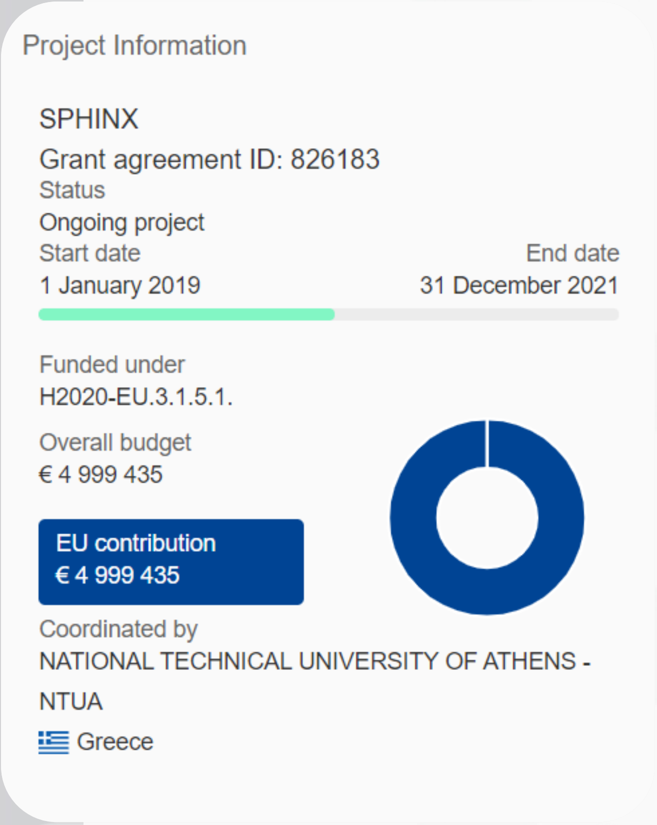
Presenter: Stylianos Karagiannis (PDMFC)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

What is SPHINX?





Project Information

SPHINX

Grant agreement ID: 826183

Status

Ongoing project

Start date
1 January 2019

End date
31 December 2021

Funded under

H2020-EU.3.1.5.1.

Overall budget

€ 4 999 435

EU contribution

€ 4 999 435

Coordinated by

NATIONAL TECHNICAL UNIVERSITY OF ATHENS - NTUA

Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

What is SPHINX?

The Challenge

Solving the Riddle of Cyber-Security protection in Healthcare IT ecosystems.

How does SPHINX tackle the challenge?

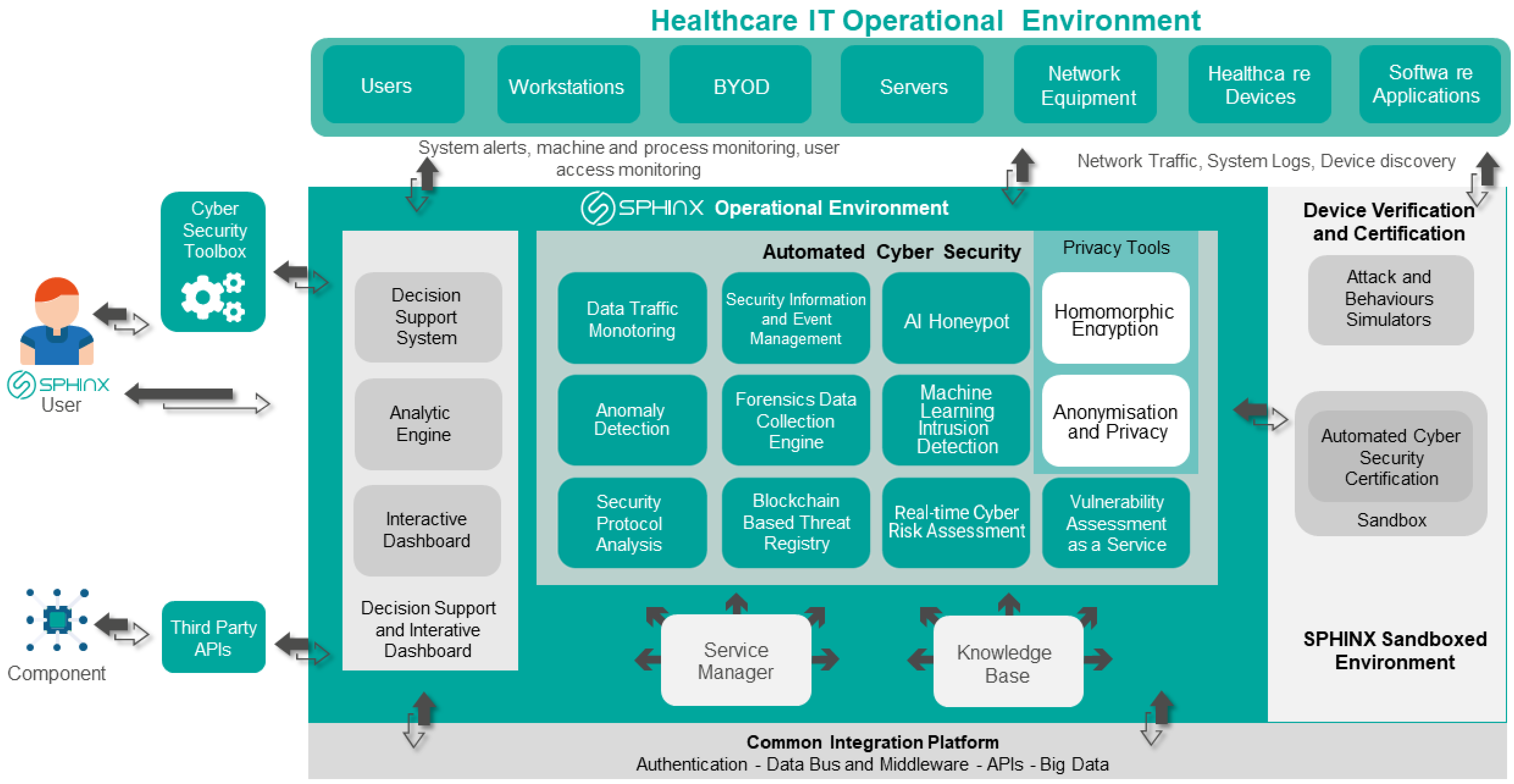
Through:

- Cyber protection and data privacy and integrity
- The proactive assessment and mitigation of Cyber-Security threats
- Evaluation of the Vulnerability of Medical Devices and Services
- Providing the SPHINX Certification
- Near real time vulnerability assessment of operating IT Ecosystems

Pilot

The SPHINX proposed technology and business framework will be demonstrated and validated under realistic operating conditions and various use case scenarios.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing



Healthcare IT Operational Environment

Users

Workstations

BYOD

Servers

Network Equipment

Healthca re Devices

Softwa re Applications

System alerts, machine and process monitoring, user access monitoring

Network Traffic, System Logs, Device discovery

SPHINX Operational Environment

Cyber Security Toolbox

SPHINX User

Component

Third Party APIs

Decision Support System

Analytic Engine

Interactive Dashboard

Decision Support and Interative Dashboard

Automated Cyber Security

Data Traffic Monotoring

Security Information and Event Management

AI Honeypot

Anomaly Detection

Forensics Data Collection Engine

Machine Learning Intrusion Detection

Security Protocol Analysis

Blockchain Based Threat Registry

Real-time Cyber Risk Assessment

Vulnerability Assessment as a Service

Privacy Tools

Homomorphic Encryption

Anonymisation and Privacy

Service Manager

Knowledge Base

Device Verification and Certification

Attack and Behaviours Simulators

Automated Cyber Security Certification

Sandbox

SPHINX Sandboxed Environment

Common Integration Platform

Authentication - Data Bus and Middleware - APIs - Big Data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

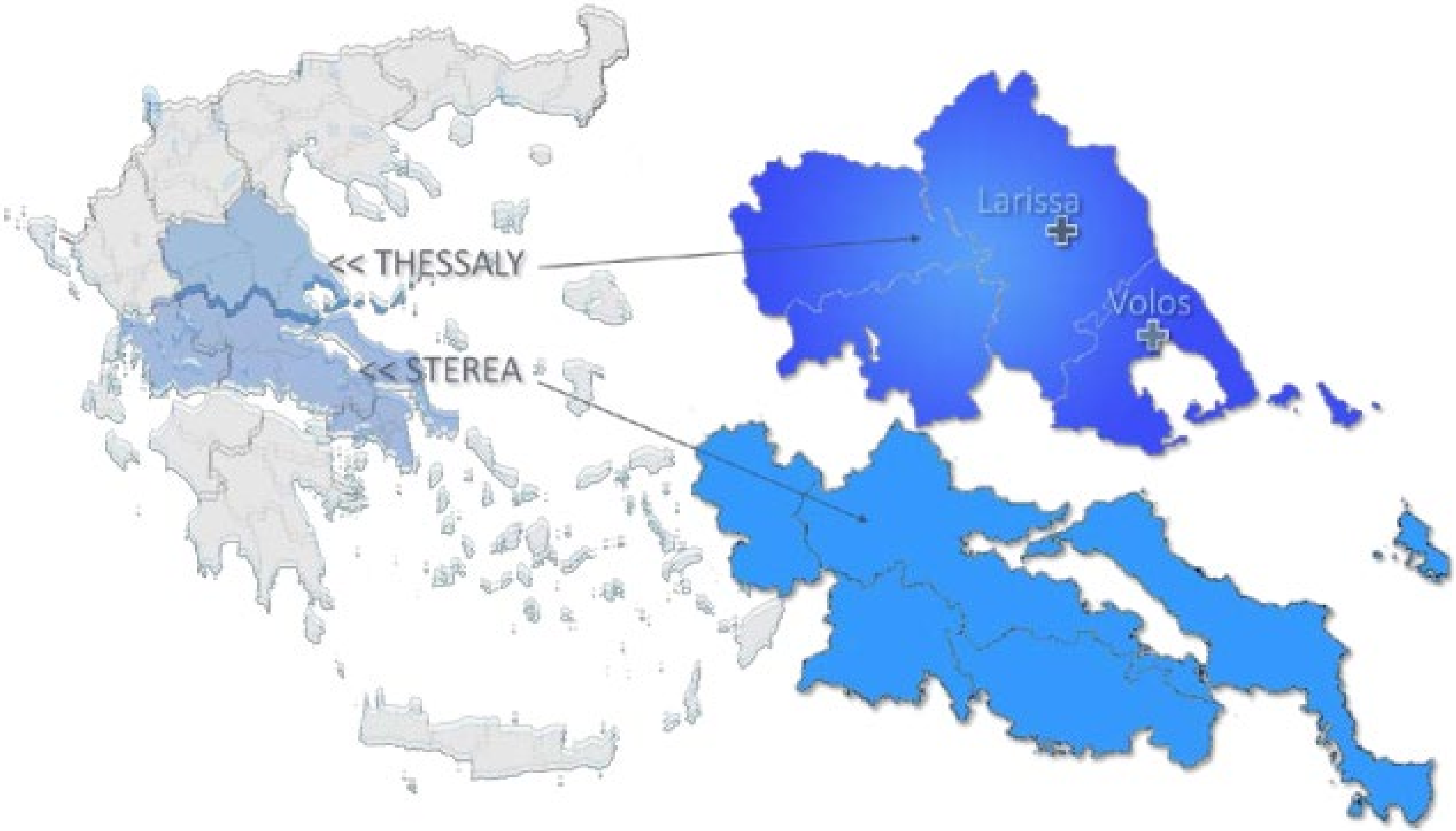
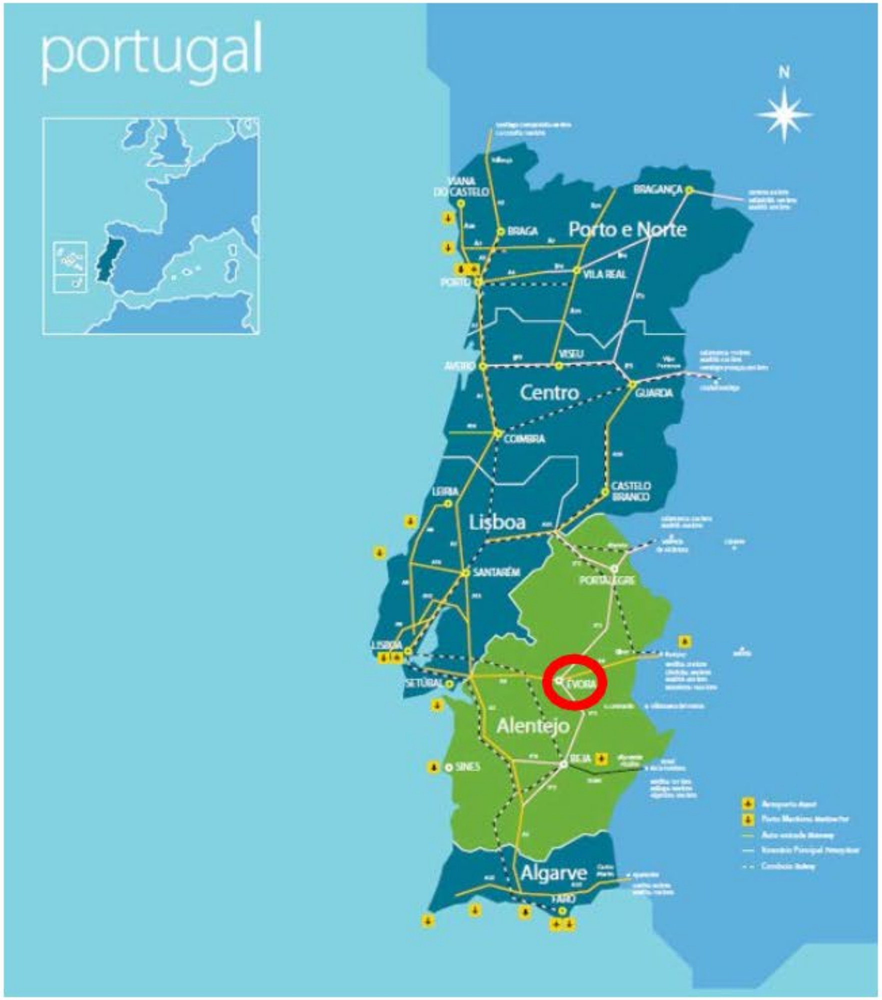


Figure 8: DYPE5's Area of Responsibility

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing



38
Medical
Specialities

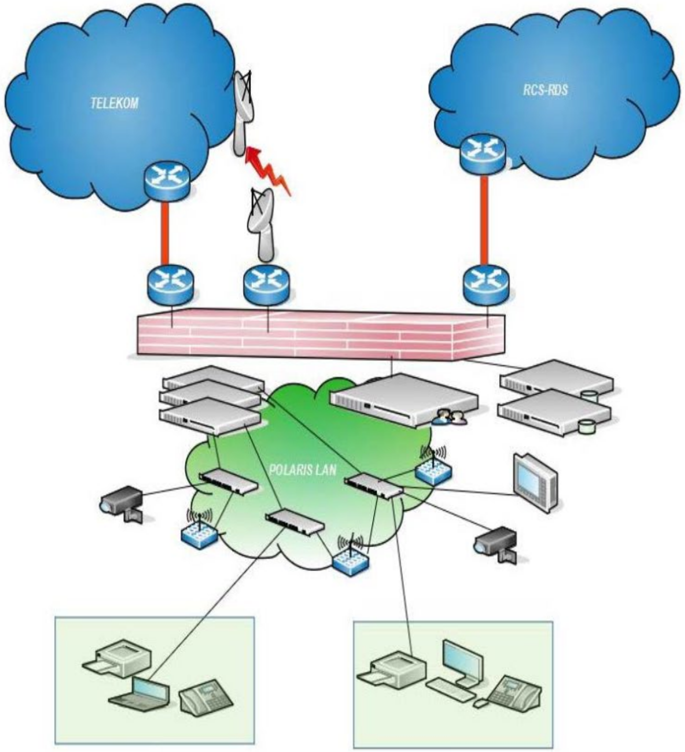
200 000
Inhabitants

Direct Coverage
Area

500 000
Inhabitants

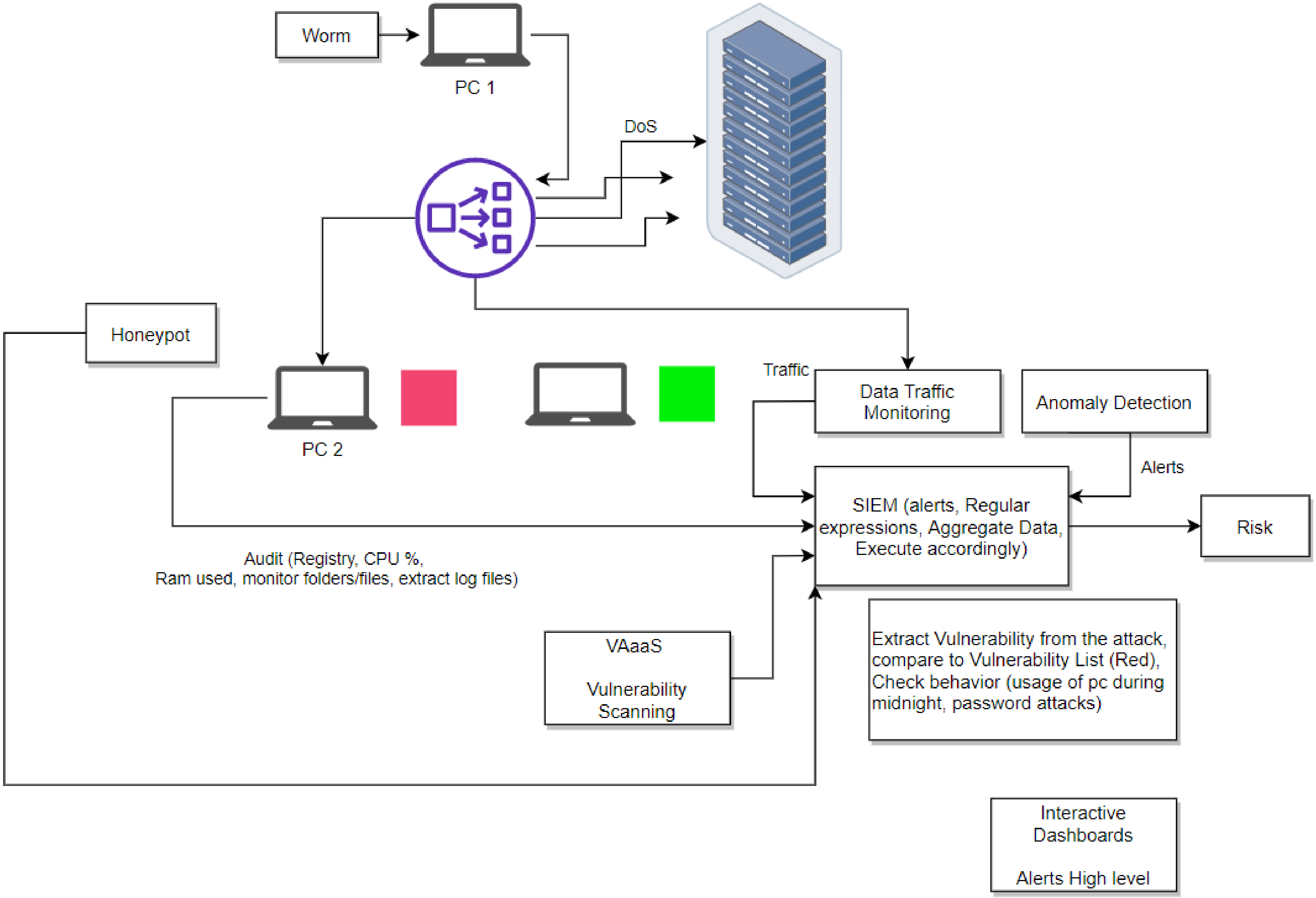
Indirect Coverage
Area

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing



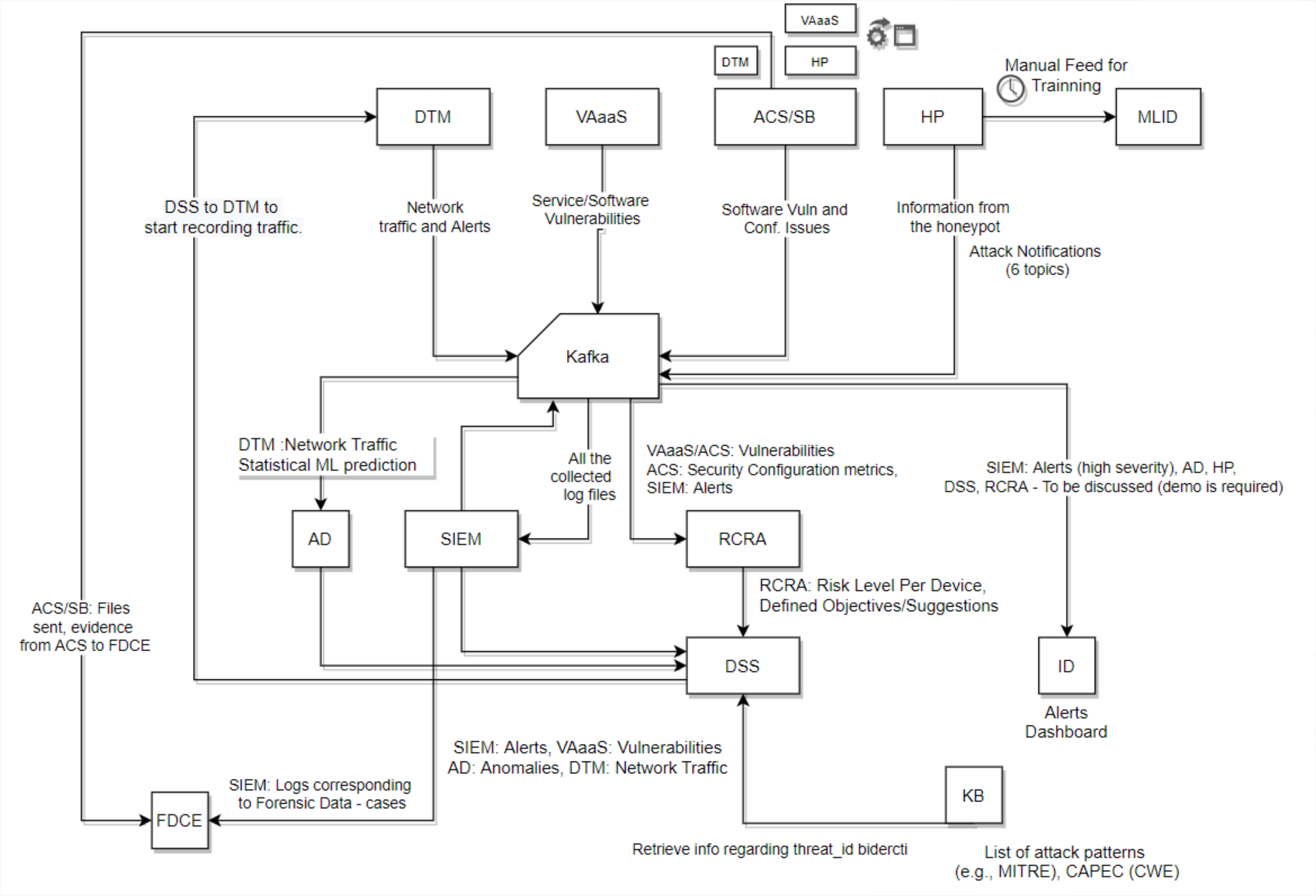
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Attack Case


Worm
PC 1
DoS
Honeypot
PC 2
Traffic
Data Traffic Monitoring
Anomaly Detection
Alerts
SIEM (alerts, Regular expressions, Aggregate Data, Execute accordingly)
Risk
Audit (Registry, CPU %, Ram used, monitor folders/files, extract log files)
VAaaS
Vulnerability Scanning
Extract Vulnerability from the attack, compare to Vulnerability List (Red), Check behavior (usage of pc during midnight, password attacks)
Interactive Dashboards
Alerts High level

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Structural Diagram (Interactions)



VAaaS

DTM

HP

DTM

VAaaS

ACS/SB

HP

MLID

Manual Feed for Trainning

DSS to DTM to start recording traffic.

Network traffic and Alerts

Service/Software Vulnerabilities

Software Vuln and Conf. Issues

Information from the honeypot

Attack Notifications (6 topics)

Kafka

DTM :Network Traffic Statistical ML prediction

All the collected log files

VAaaS/ACS: Vulnerabilities
ACS: Security Configuration metrics,
SIEM: Alerts

SIEM: Alerts (high severity), AD, HP,
DSS, RCRA - To be discussed (demo is required)

AD

SIEM

RCRA

RCRA: Risk Level Per Device,
Defined Objectives/Suggestions

ACS/SB: Files sent, evidence from ACS to FDCE

DSS

ID

Alerts Dashboard

SIEM: Alerts, VAaaS: Vulnerabilities
AD: Anomalies, DTM: Network Traffic

SIEM: Logs corresponding to Forensic Data - cases

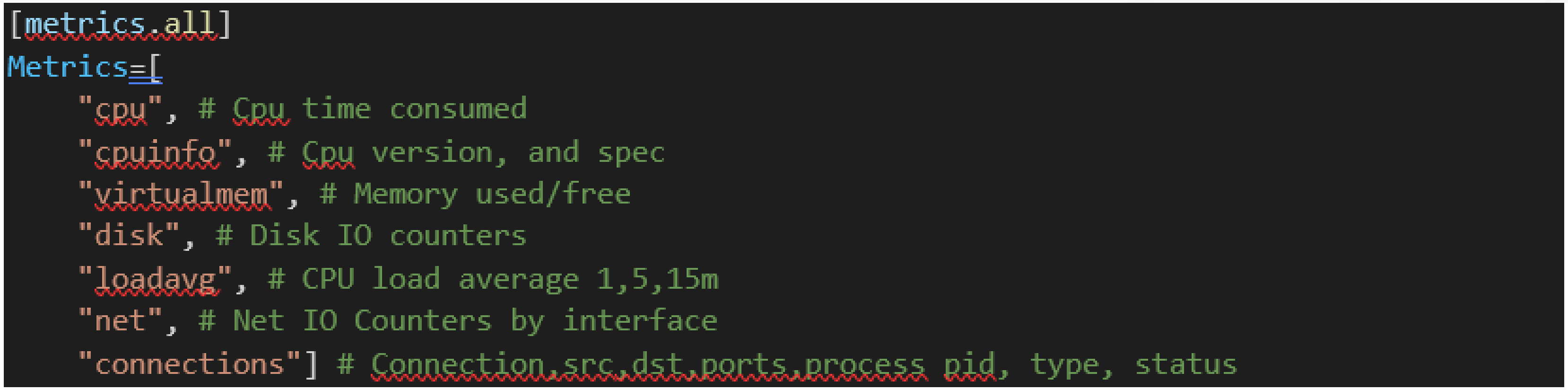
FDCE

KB

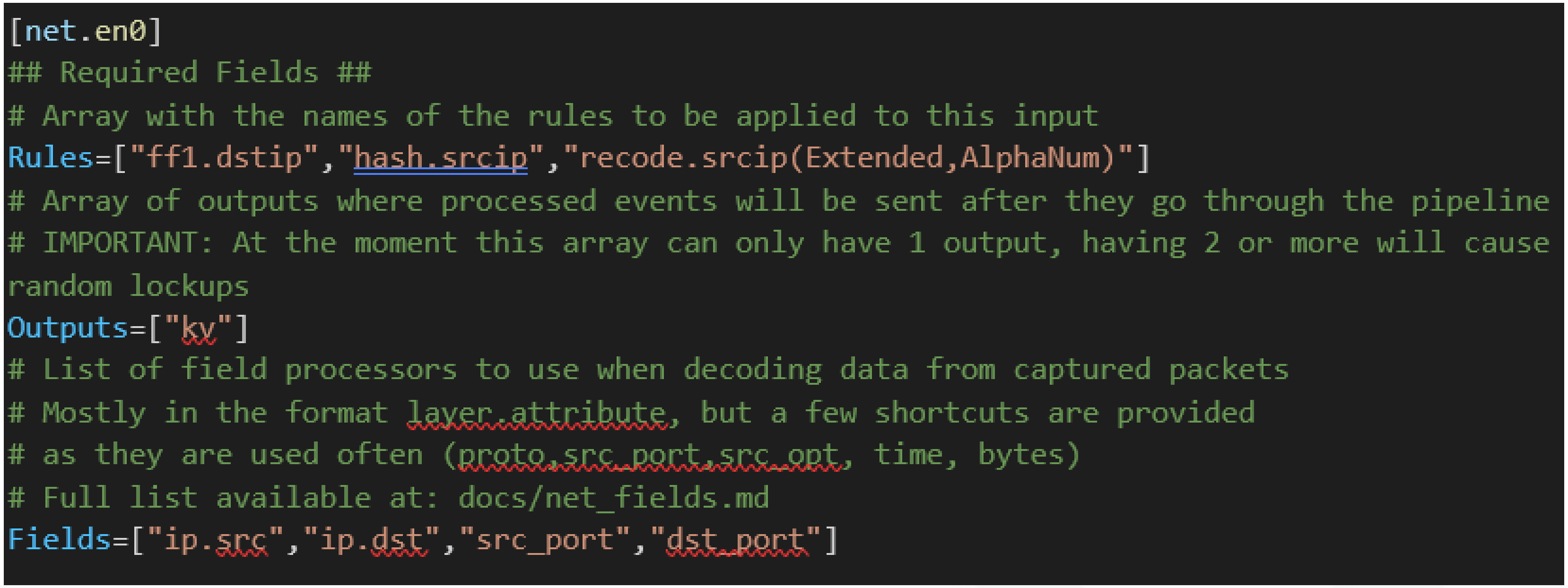
Retrieve info regarding threat_id bidercti

List of attack patterns
(e.g., MITRE), CAPEC (CWE)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing



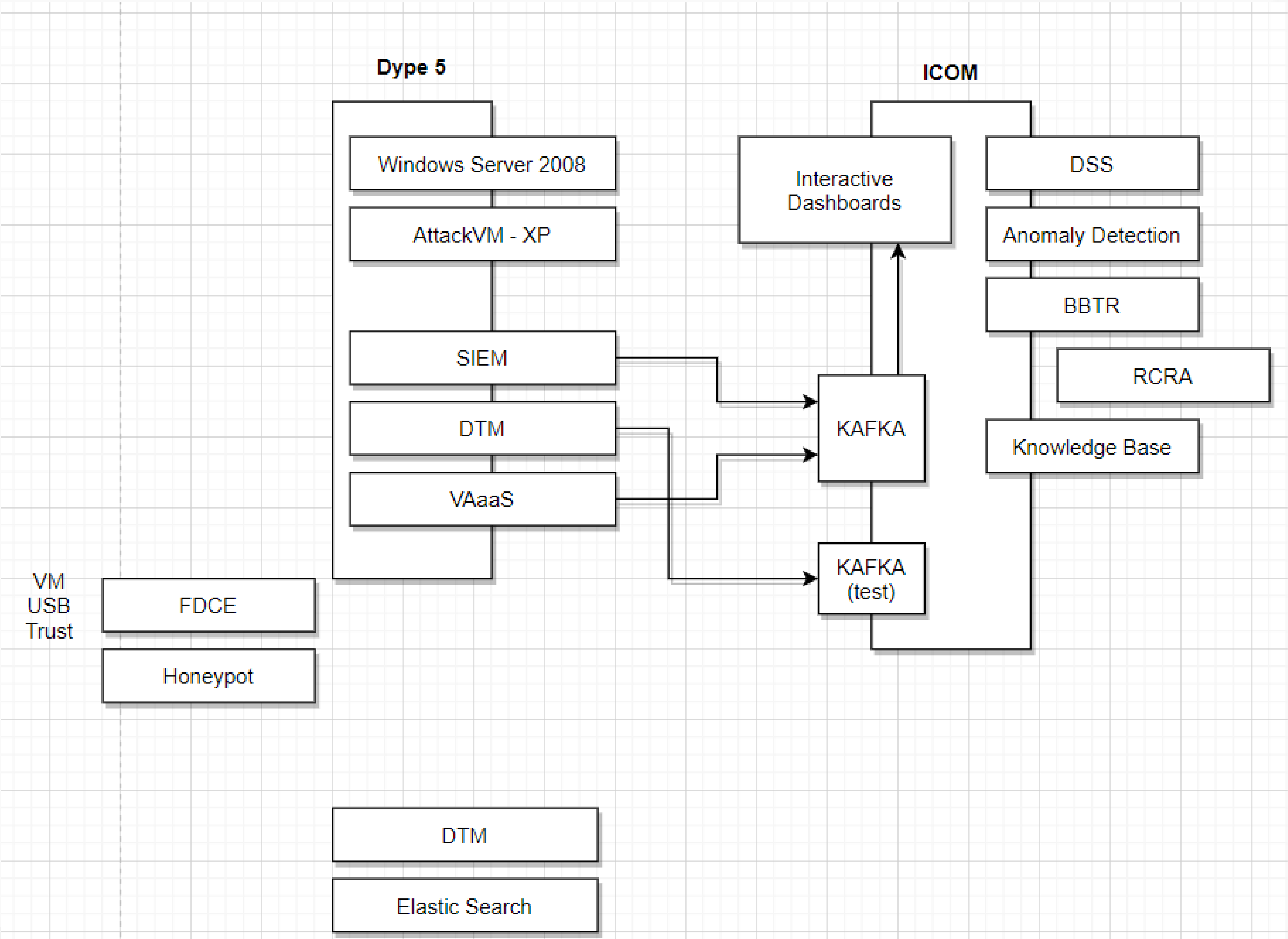
```
[metrics.all]
Metrics=[
    "cpu", # Cpu time consumed
    "cpuinfo", # Cpu version, and spec
    "virtualmem", # Memory used/free
    "disk", # Disk IO counters
    "loadavg", # CPU load average 1,5,15m
    "net", # Net IO Counters by interface
    "connections"] # Connection,src,dst,ports,process pid, type, status
```



```
[net.en0]
## Required Fields ##
# Array with the names of the rules to be applied to this input
Rules=["ff1.dstip","hash.srcip","recode.srcip(Extended,AlphaNum)"]
# Array of outputs where processed events will be sent after they go through the pipeline
# IMPORTANT: At the moment this array can only have 1 output, having 2 or more will cause random lockups
Outputs=["kv"]
# List of field processors to use when decoding data from captured packets
# Mostly in the format layer.attribute, but a few shortcuts are provided
# as they are used often (proto,src_port,src_opt, time, bytes)
# Full list available at: docs/net_fields.md
Fields=["ip.src","ip.dst","src_port","dst_port"]
```

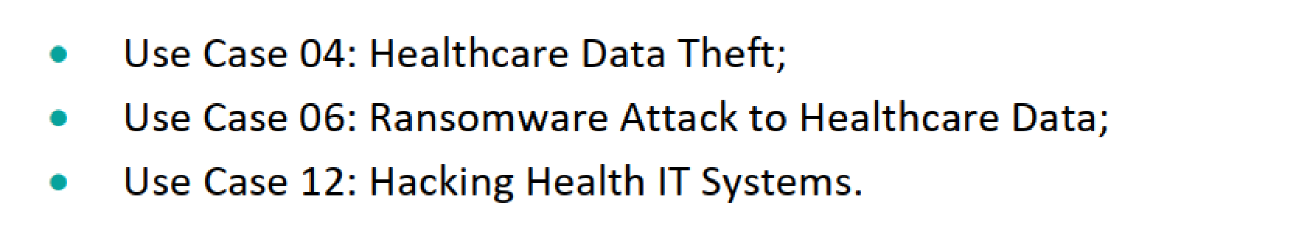
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Topology / Sphinx Deployment

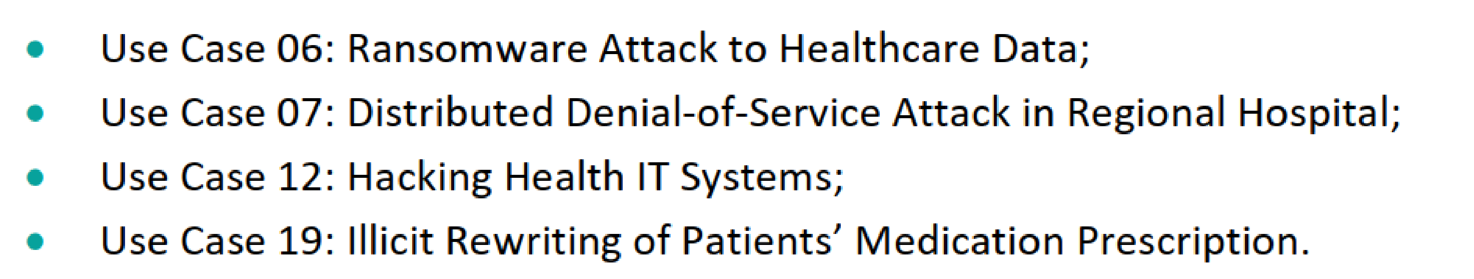


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

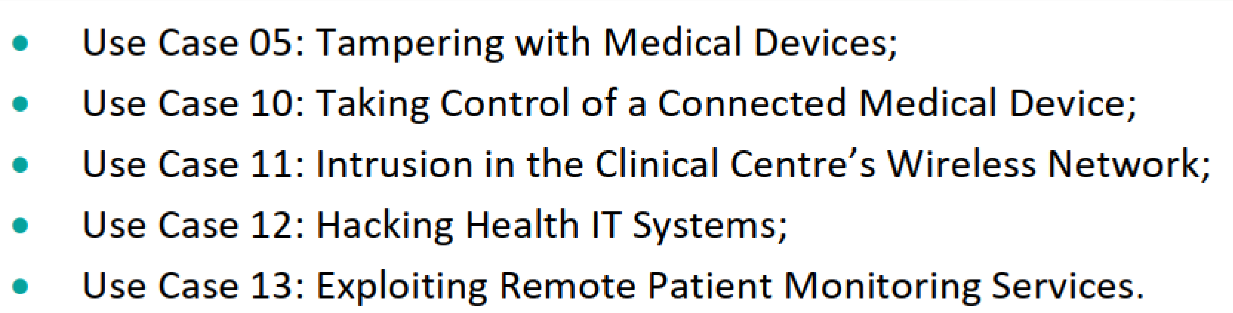
Use Cases from Pilots



- Use Case 04: Healthcare Data Theft;
- Use Case 06: Ransomware Attack to Healthcare Data;
- Use Case 12: Hacking Health IT Systems.



- Use Case 06: Ransomware Attack to Healthcare Data;
- Use Case 07: Distributed Denial-of-Service Attack in Regional Hospital;
- Use Case 12: Hacking Health IT Systems;
- Use Case 19: Illicit Rewriting of Patients’ Medication Prescription.



- Use Case 05: Tampering with Medical Devices;
- Use Case 10: Taking Control of a Connected Medical Device;
- Use Case 11: Intrusion in the Clinical Centre’s Wireless Network;
- Use Case 12: Hacking Health IT Systems;
- Use Case 13: Exploiting Remote Patient Monitoring Services.

Use Cases	Attack Vector	Missing tasks, component	Main Mitigation
UC1: Attacking Obsolete Operating Systems in Hospital	Conficker SMB, old systems vulns	~~Network Isolation is missing~~	Network Traffic, Signatures
UC2: Hijacking Access to National Healthcare Databases	Network scanning, Bruteforce credentials	aDSL router Wi-Fi required	SIEM, Network Traffic
UC3: Rootkit Malware Attack in a Cancer Treatment Institute	Rootkit from Emails, Remote Website Connection	Check if Mailserver (NTUA) works	Signature, Network Traffic
UC4: Theft of Health Data by Exploiting Vulnerable Software	Malware executable, Emails		Signature, Network Traffic
UC5: Tampering with Medical Devices	USB - Virus	Connect USB - virus to medical devices - Certification / Auditing	Not identified/Discussion
UC6: Ransomware Attack to Healthcare Data	Cryptolocker - Emotet	~~Network Isolation is missing~~	Signature, Network Traffic
UC7: Distributed Denial-of-Service Attack in Regional Hospital	DDoS	Check compatibility with Fortigate	Network Traffic
UC8: Compromising Health Services through Cryptocurrency Mining	Cryptomining		Signature, Network Traffic, System Performance (SIEM)
UC9: Compromised BYOD Enables Stealing of Patient Data	Malware on Android, steal doctor's credentials	Tablet is required	Network Traffic, Signatures
UC10: Taking Control of Connected Medical Devices	nation attack tools + SQL injection + Remote shell -> RDP	OWASP maybe for SQL injection	Behavior analysis
UC11: Intrusion in the Clinical Centre’s Wireless Network	WPA2 cracker + weak admin password	Wifi Required	Network Traffic, SIEM, AP status
UC12: Hacking Health IT Systems	Nmap, Vulnscan		Network Traffic, ACS
UC13: Exploiting Remote Patient Monitoring Services	Wi-Fi intrusion, HTTP vs HTTPS, sniffing, VPNFilter at Router	How VPNFilter works	Network Traffic, ACS
UC14: Zero Day Attack to eHealth Services	Zero-Day Attack	Create Zero Day	Network traffic, Integrity changes, SIEM
UC15: Theft of Hospital Equipment	Old authorized device is used	Add list of current MAC addresses (SIEM), Asset Management (RCRA)	Behavior analysis, Old device is reused - Login, Network Traffic

Best Practices

1. Always use SSD: Performance is very important, at least the main services must be executed by using SSD. Virtual Machines are ultra fast that way.
2. RAM (24GB to 512GB ++): Elastic Search and other similar data storage/indexing uses a lot of RAM (fast search and log indexing). Elastic Search (8GB RAM). DTM/AD (8GB RAM)
3. Scalability - SSD Capacity depends on the log files: The storage and capacity requirements might get big depending on the logs and the size of the infrastructure.
4. K8s for continuous Integration/Updates: Deploying Kubernetes is a good practice even if it is harder approach.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Best Practices (2)

1. Docker for simple and portable deployments: It is possible to deploy some of the service individually.
2. Kafka Server to be deployed: This is the main information feeder to connect the microservices.
3. VM Hypervisor to select (VMWare, Proxmox, Terraform): It is important to select the best according to needs and requirements.
4. Interactive Dashboards important for the end user.
5. Create alerts and checks according to needs: Important step to test the deployment.
6. Set DTM accordingly and other components to subnets, configure SIEM etc.
7. Ready to attack and defend

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Installation Steps

1. Select VM Hypervisor for Master and Worker
2. Deploy Kubernetes and Workers
3. Deploy Kafka
4. Deploy Services
5. Deploy VMs (Required for FDCE, Sandbox, Attack Simulation, Honeypots)
6. Configure services to interact with Kafka
7. Configure what to monitor (subnets, auditing, log files etc.)
8. Execute test scenarios
9. Iteratively check and configure rules, check vulnerabilities and respond to the Incident Response plan

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Kubernetes Deployment

1. Install Docker
2. Start and Enable Docker
3. Add Kubernetes Signing Key
4. Add Software Repositories
5. Kubernetes Installation Tools kubeadm - repeat for each server node
6. Disabling the swap sudo swapoff –a
7. Assign Unique Hostname for Each Server Node (master and workers)
8. Initialize Kubernetes on Master Node
9. Deploy Pod Network to Cluster
10. Join Worker Node to Cluster
11. Get Nodes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Benefits from the Approach

Its hard but its worth it

1. Get familiar with rather novel tools that only presented in theory
2. Test the existing environment
3. Educate IT staff not only on security but in automated tasks and novel methods of DevOps and SecDevOps
4. Increase security awareness (capability to replicate scenarios according to the business processes)
5. Improve the infrastructure (Backup plans etc)
6. Increase situational awareness (know where is what)
7. Define better security protocols to be followed (identity management, authentication schemes, privacy)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Thank you

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing