Panacea
People-centric cybersecurity in healthcare

PANACEA Dynamic Risk Management Platform

Fabrizio De Vecchis
RHEA
Silvia Bonomi
UROME

DRMP Workshop
15 September 2020

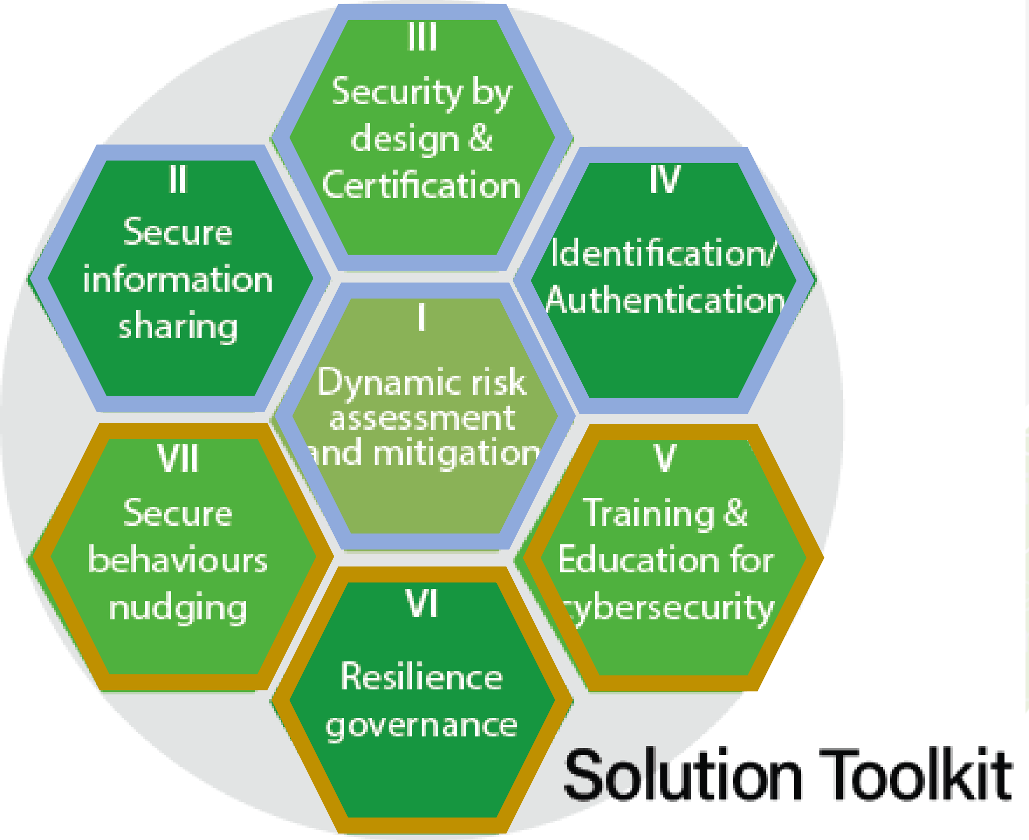
Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

Agenda

- Solution Toolkit
- DRMP Concept
- DRMP Innovation Point
- DRMP Status
- DRMP Use Cases
- DRMP High-Level Design
- DRMP Function & Data
- DRMP Computation Flow
- DRMP Emulation Environment

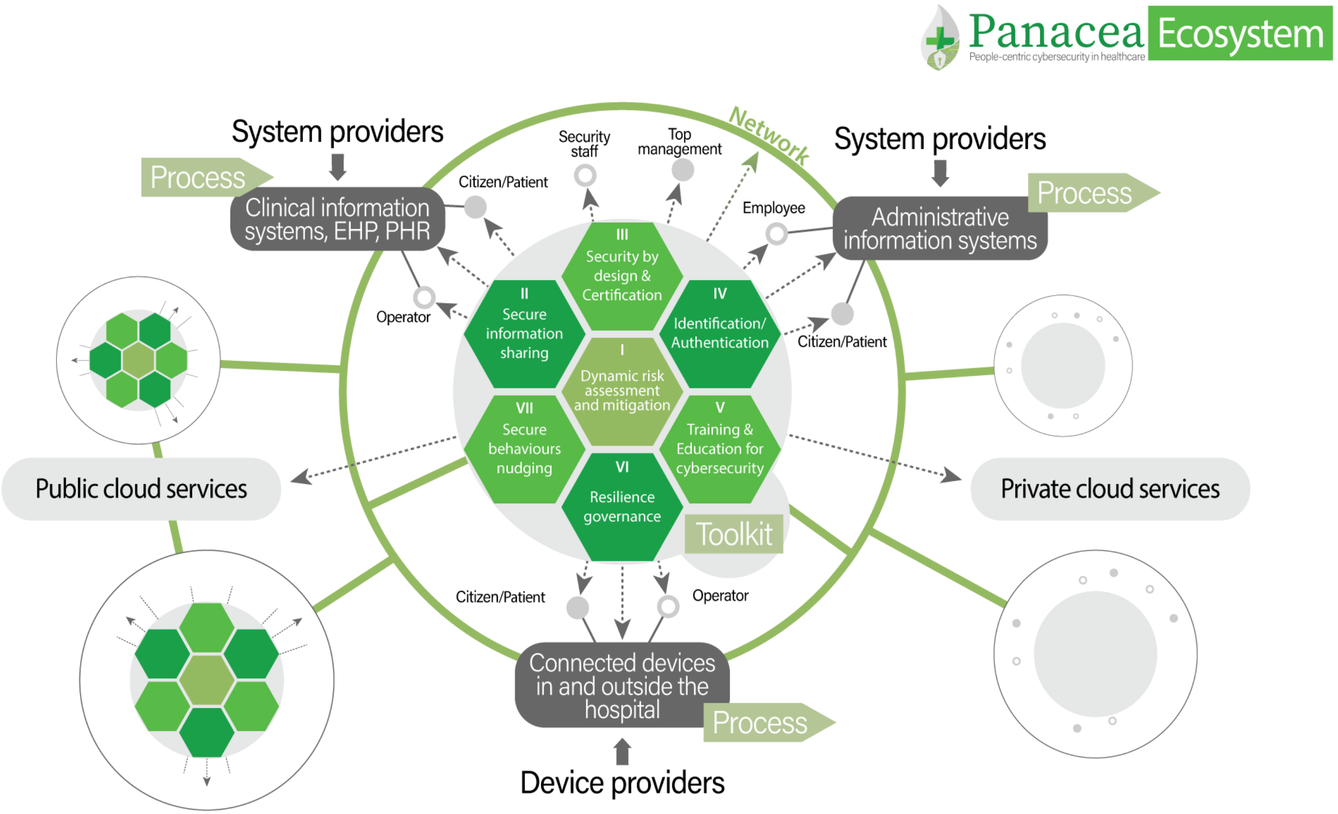
PANACEA Solution Toolkit

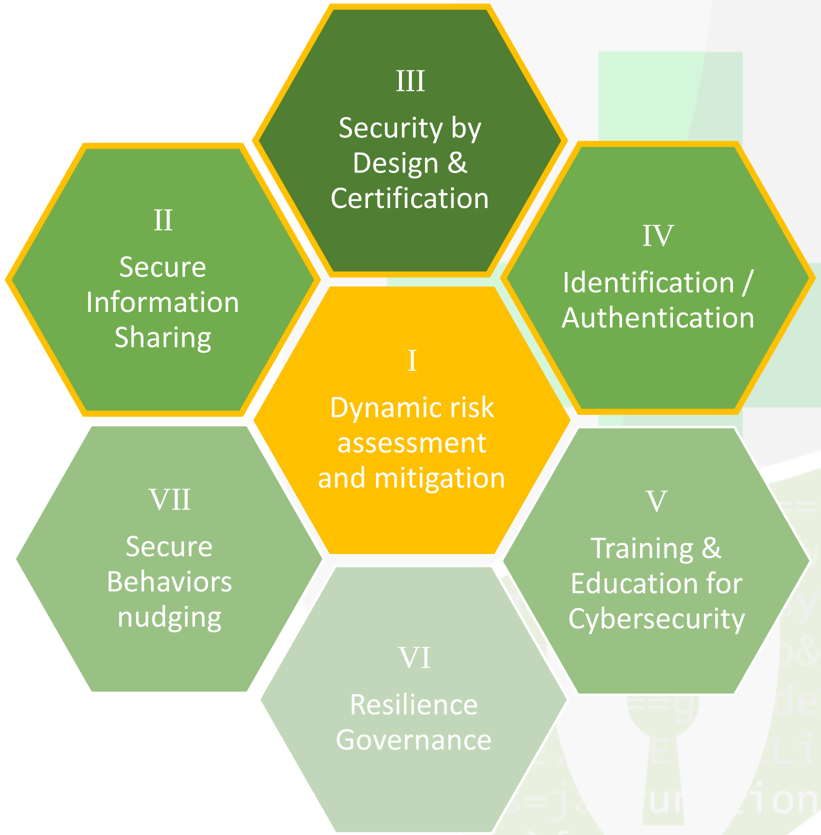
- The **PANACEA Toolkit** includes
  - **four technological tools** for
    - I-dynamic risk assessment & mitigation,
    - II-secure information sharing,
    - III-security-by-design & certification,
    - IV-identification & authentication
  - **three organisational tools** for
    - V-training & education,
    - VI-resilience governance,
    - VII-secure behaviours nudging


III
Security by design & Certification
II
Secure information sharing
IV
Identification/ Authentication
I
Dynamic risk assessment and mitigation
VII
Secure behaviours nudging
V
Training & Education for cybersecurity
VI
Resilience governance
Solution Toolkit

Solution Toolkit - DRMP

- **Dynamic Risk Management Platform (DRMP), a technological tool of the PANACEA Solution Toolkit**


Panacea Ecosystem
People-centric cybersecurity in healthcare
System providers
Process
Clinical information systems, EHP, PHR
Security staff
Top management
Network
System providers
Process
Administrative information systems
Citizen/Patient
Employee
Operator
Citizen/Patient
III
Security by design & Certification
II
Secure information sharing
IV
Identification/ Authentication
I
Dynamic risk assessment and mitigation
VII
Secure behaviours nudging
V
Training & Education for cybersecurity
VI
Resilience governance
Toolkit
Public cloud services
Private cloud services
Citizen/Patient
Operator
Connected devices in and outside the hospital
Process
Device providers


III
Security by Design & Certification

II
Secure Information Sharing

IV
Identification / Authentication

I
Dynamic risk assessment and mitigation

VII
Secure Behaviors nudging

V
Training & Education for Cybersecurity

VI
Resilience Governance

GA Concept for DRMP

Objective 1: Develop and validate tools for dynamic risk assessment and mitigation

In order to increase the cyber security resilience of the IT infrastructure of the HCCs, the PANACEA project will define new models able to **rapidly capture and analyze the multiple variables involved in a potential attack, ranging from business, to human, to technical aspects.**

DRMP aims to proactively protect a complex IT infrastructure (encompassing remote and IoT devices, remote networks, local networks) by quantitatively analyzing the current level of risk given a multi-dimensional threat analysis and the current business impact (with quantitative dependencies between assets and business processes). The computation of the risk will trigger the definition of mitigation actions (security measures) with the purpose of reducing the level of risk but containing the business impact that the actions themselves may cause. The platform will leverage and propose both technical (i.e. precise actions on the IT infrastructure, from patching to architectural/configuration) and non-technical (organizational, procedural) security measures.

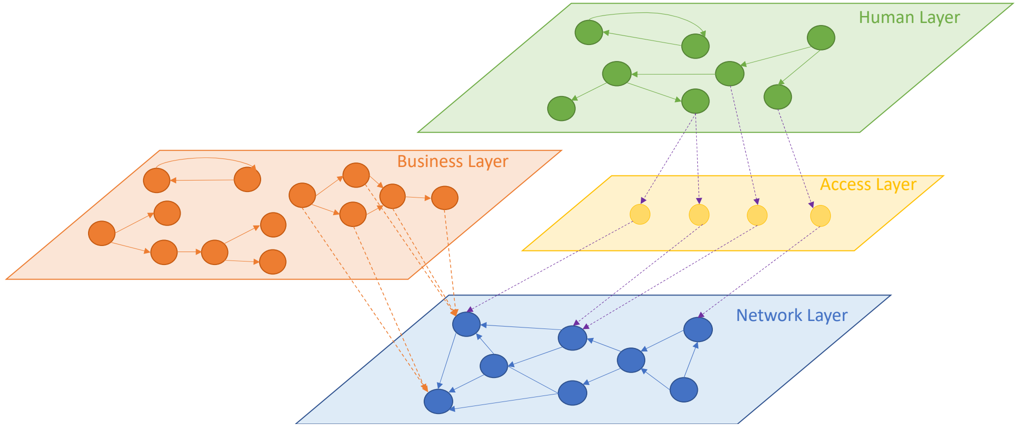
DRMP is supported by:

- **Visual analytic environment**: to help security operators to effectively visualize and process results
- **Business impact computation**, based on the dependencies between IT assets and related business processes
- **Heterogeneous data collection and information storage**: the project will develop various types of connectors to manage transfer and normalization of data from different internal and external sources. It will also set up forensically sound ways for storing the data.
- **Data aggregation, organization and analysis**, also using statistical techniques such as permutation entropy. to describe an organization in term of business process; security process; network and application topology.
- **a Knowledge Base of Threats and Attack Strategies**, in terms of types of threats, type of tools, and types of techniques known at a given moment.

The risk assessment tools will be integrated with a tool capable to recommend and rank appropriate mitigation actions, both technical and organizational.

DRMP – Innovation Points

- A novel multi-dimensional attack model i.e., *multi-layer attack graph*
  - It is able to represent relationships between people, ICT and medical devices, business processes and access rights to the system.
  - It is a vulnerability-based model i.e., the focus is representing vulnerabilities affecting the system, their possible exploits and emerging chains of exploits leading to a multi-step attack.
  - It will be the base the risk identification and quantification process.
  - It will be validated trough the instantiation in the DRMP identified user scenarios.

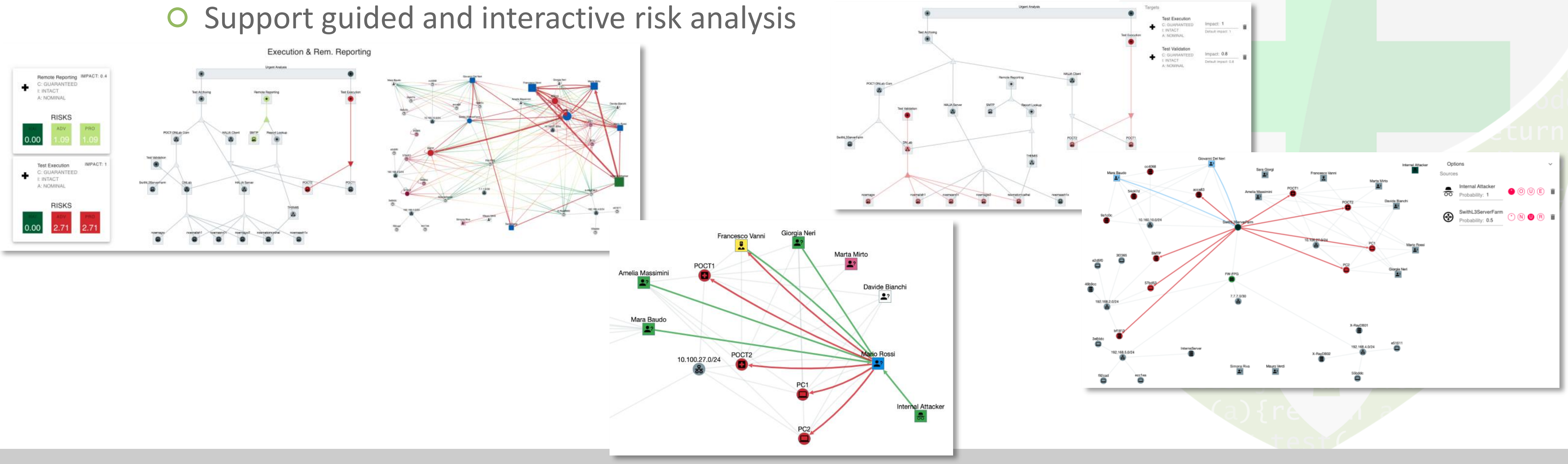


DRMP – Innovation Points

- Semi-automatic identification of response actions at both technical and non-technical level to reduce organization risk.
  - Most of the automated solutions only consider technical actions
    - e.g., closing a port on a device, changing firewall rules, switching off devices etc.
  - PANACEA will combine both technical and non-technical mitigation actions to generate a comprehensive response plan
  - Response plans will be generated by solving a multi objective optimization problem

DRMP – Innovation Points

- An innovative visual analytics environment
  - Support security operators with increased situational awareness
  - Support the analysis and interaction with the multi-layer attack graph
  - Support guided and interactive risk analysis



Remote Reporting IMPACT: 0.4
C: GUARANTEED
I: INTACT
A: NOMINAL

RISKS

HAI	ADV	PRO
0.00	1.09	1.09

Test Execution IMPACT: 1
C: GUARANTEED
I: INTACT
A: NOMINAL

RISKS

HAI	ADV	PRO
0.00	2.71	2.71

Targets

Test Execution
C: GUARANTEED
I: INTACT
A: NOMINAL
Impact: 1
Default impact: 1

Test Validation
C: GUARANTEED
I: INTACT
A: NOMINAL
Impact: 0.8
Default impact: 0.8

Options

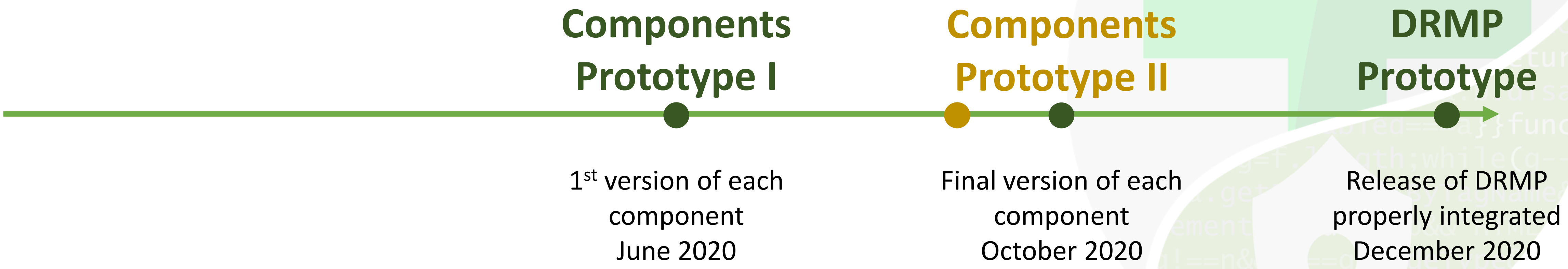
Sources

Internal Attacker
Probability: 1

SwithL3ServerFarm
Probability: 0.5

DRMP Development Status

Components development status compared to the next releases of the platform.



Components Prototype I

1st version of each component
June 2020

Components Prototype II

Final version of each component
October 2020

DRMP Prototype

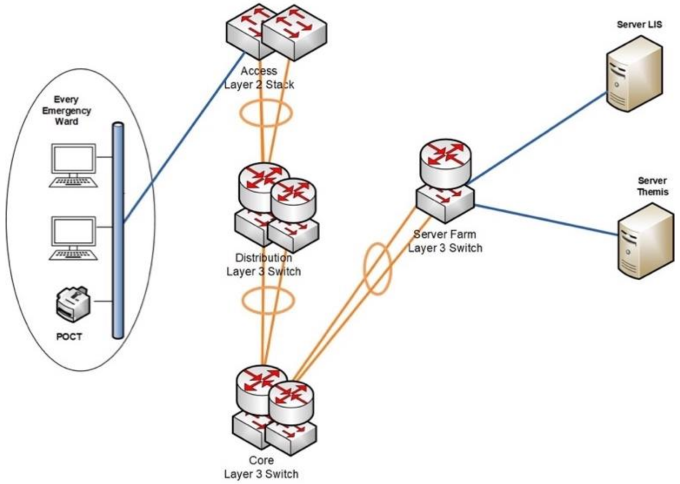
Release of DRMP properly integrated
December 2020

Planned Use Cases

User scenario 1: FPG-LIS and connected POCTs

This scenario focuses upon sharing of data between the Laboratory Information System (LIS) and the Point Of Care Testing (POCT) medical devices, during an **'urgent analysis' process**. POCT (or bedside testing) is defined as a medical diagnostic testing at or near the point of care – that is, at the time and place of patient care (such as the patients' bedside). POCT is performed through connected medical devices. There are 20 networked POCT devices. This scenario refers to the **use of the blood gas analyzer**.

Actors include those in the lab and those in two departments using the POCTs.

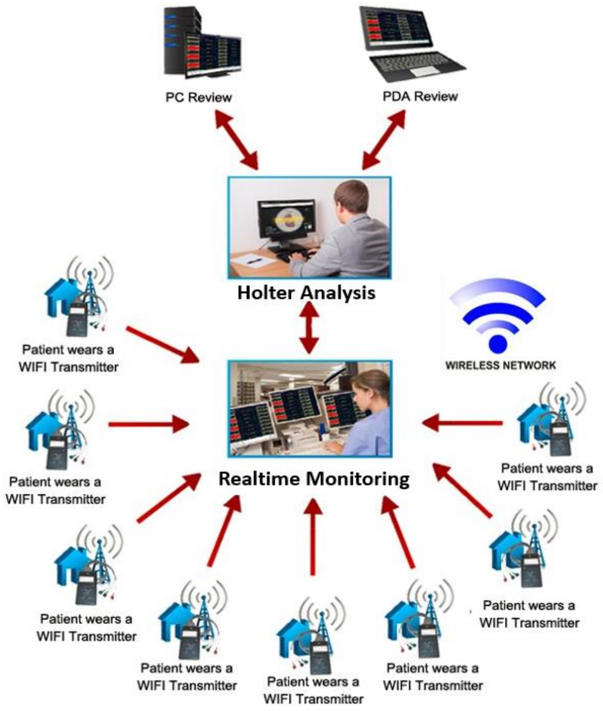


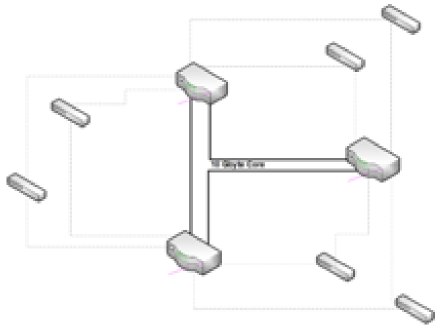
Ready in Emulation Environment

Planned Use Cases

User scenario 5: HSE Connected Medical Devices

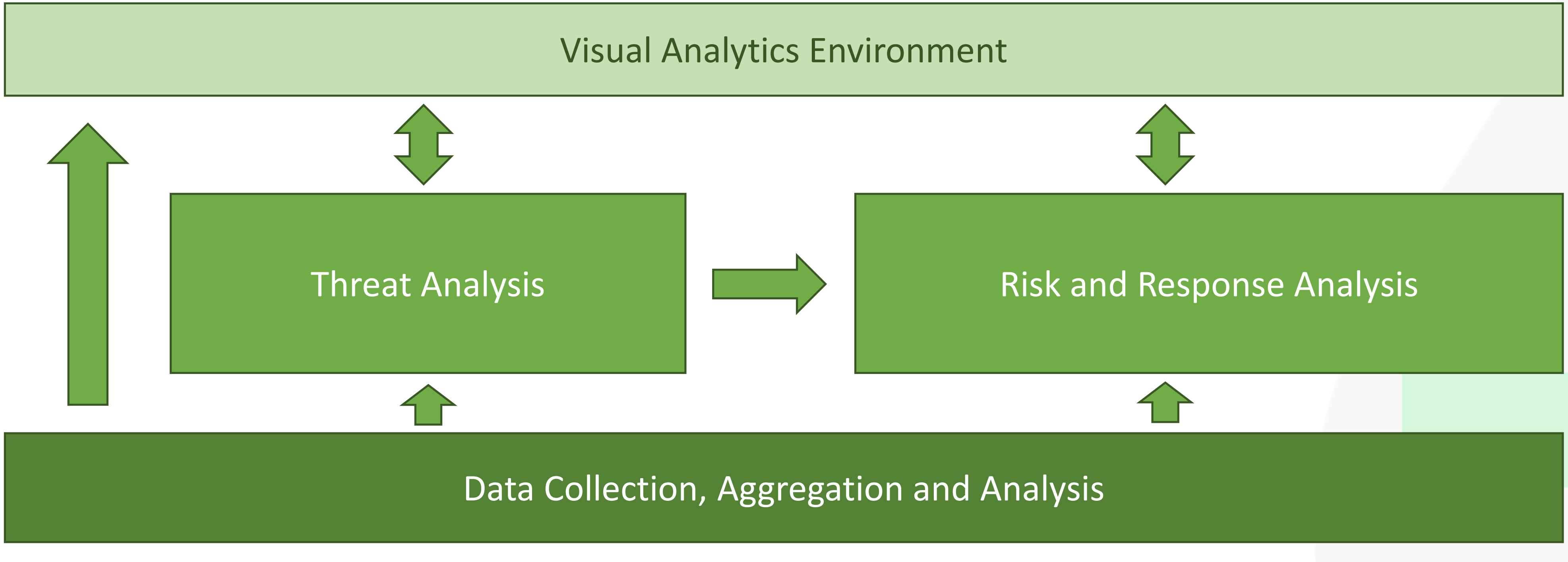
This scenario regards the use of two devices: (i) a wireless telemetry device (Holter monitor) connected through a dedicated wireless network to a telemetry management and monitoring system monitored from within Critical Care Unit (CCU); patients using the wireless monitoring solution are geographically placed across a number of medical wards throughout the hospital; (ii) an ultrasound machine operating within a radiology department through a fixed cable connection to the hospital infrastructure.


PC Review
PDA Review
Holter Analysis
WIRELESS NETWORK
Realtime Monitoring
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter
Patient wears a WIFI Transmitter

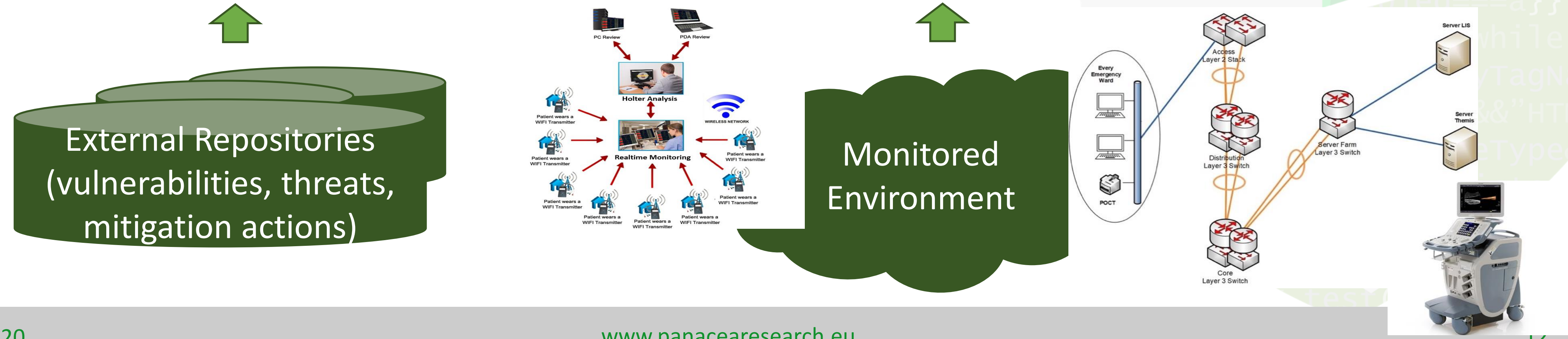


Emulation Environment on going

Dynamic Risk Management Platform (DRMP)


Visual Analytics Environment
Threat Analysis
Risk and Response Analysis
Data Collection, Aggregation and Analysis

- **Dynamic Risk Assessment and Mitigation for complex network infrastructure**

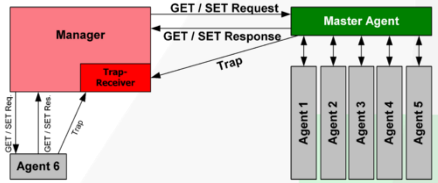


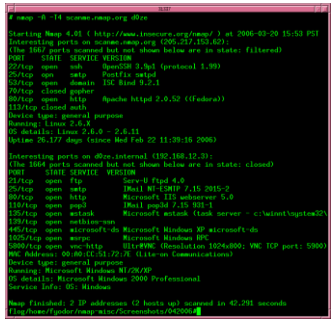
DRMP - Internal/External Data Sources

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE



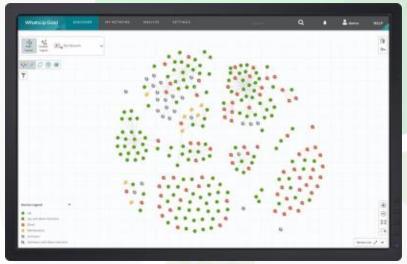


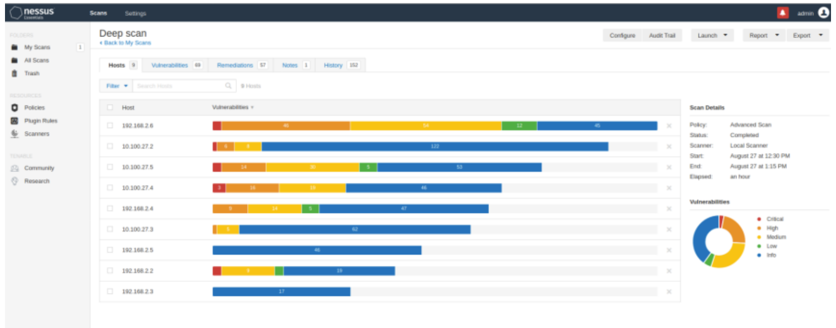
```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```





Deep scan

< Back to My Scans

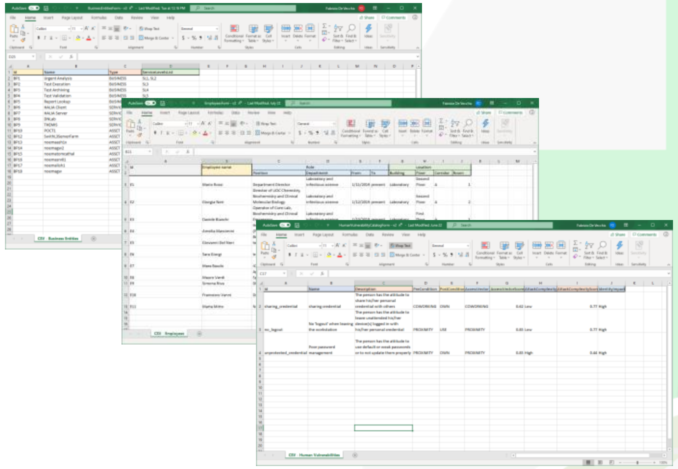
Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: August 27 at 12:30 PM
End: August 27 at 1:15 PM
Elapsed: an hour

Panacea
People-centric cybersecurity in healthcare

DRMP - Internal/External Data Sources

- Business Dependency Graph
- Employees and Credentials
- Human Policies and Human Vulnerabilities
- Cyber Security Profiles
- Pre-defined Mitigation Actions



Id	Name	Type	ServiceLevelsList
BP1	Urgent Analysis	BUSINESS	SL1, SL2
BP2	Test Execution	BUSINESS	SL3
BP3	Test Archiving	BUSINESS	SL4
BP4	Test Validation	BUSINESS	SL5
BP5	Report Lookup	BUSIN	
BP6	WALIA Client	SERVIC	
BP7	WALIA Server	SERVIC	
BP8	DNLab	SERVIC	
BP9	TMDMS	SERVIC	
BP10	POCT1	ASSET	
BP12	Switch_ServerFarm	ASSET	
BP13	noemaeth0x	ASSET	
BP14	noemapc2	ASSET	
BP15	noematomcathal	ASSET	
BP16	noemasrv01	ASSET	
BP17	noemaliohl	ASSET	
BP18	noemapc	ASSET	

CSV - Business Entities

Id	Employee name	Role				Location			
		Position	Department	From	To	Building	Floor	Corridor	Room
E1	Mario Rossi	Department Director	Laboratory and infectious science	1/11/2019	present	Laboratory	Second Floor	A	1
E2	Giorgia Neri	Director of UOC Chemistry, Biochemistry and Clinical Molecular Biology	Laboratory and infectious science	1/12/2019	present	Laboratory	Second Floor	A	2
E3	Daniele Bianchi	Operator of Core Lab, Biochemistry and Clinical Emergency	Laboratory and infectious science	1/13/2019	present	Laboratory	First Floor	A	3
E4	Amelia Mancini								
E5	Giovanni Del Neri								
E6	Sara Giorgi								
E7	Mara Rosolo								
E8	Mauro Verdi								
E9	Simona Riva								
E10	Francesco Varvo								
E11	Maria Mitto								

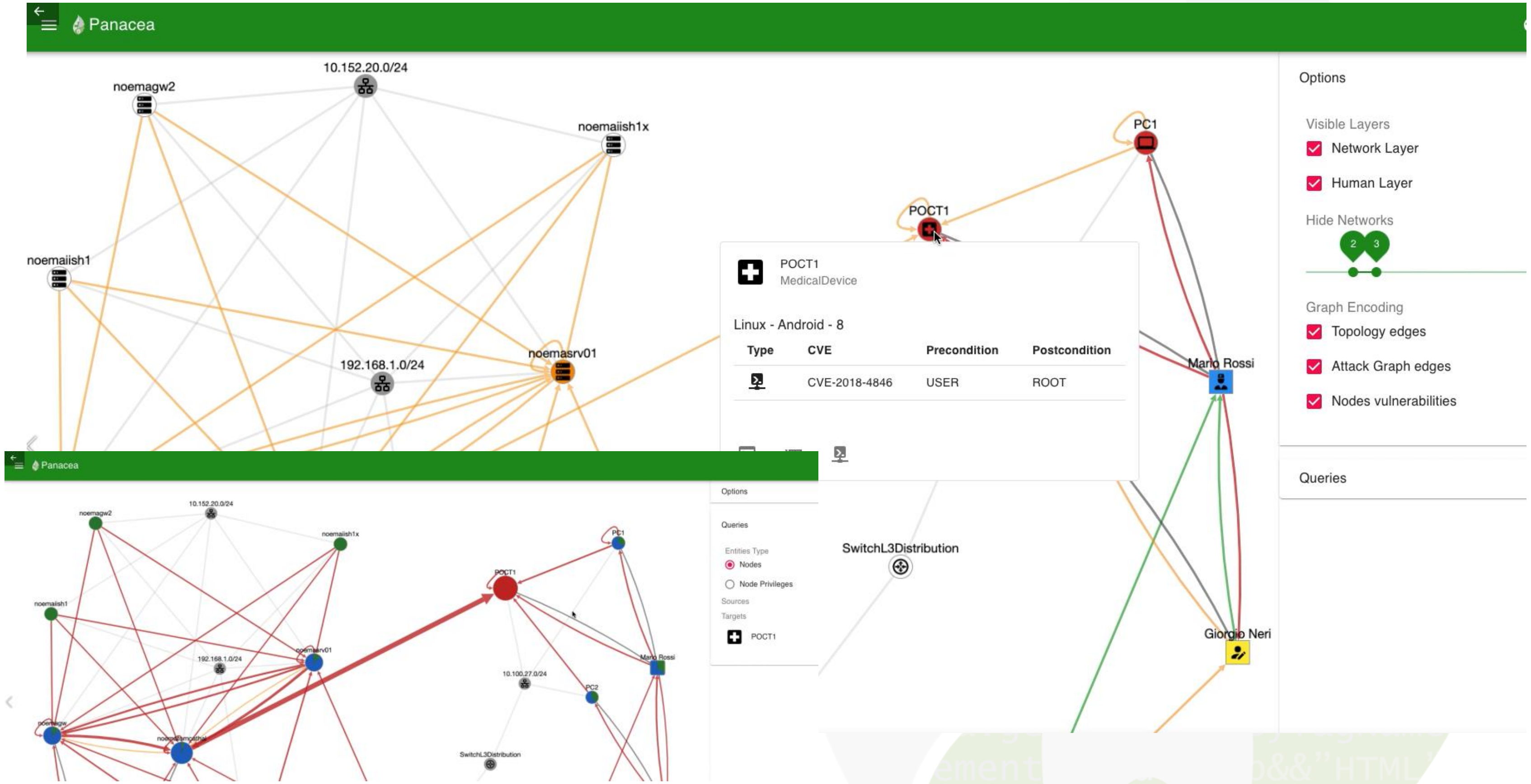
CSV - Employees

Id	Name	Description	PreCondition	PostCondition	AccessVector	AccessVectorScore	AttackComplexity	AttackComplexityScore	IdentityImpact
sharing_credential	sharing credential	The person has the attitude to share his/her personal credential with others	COWORKING	OWN	COWORKING	0.62	Low	0.77	High
no_logout	No "logout" when leaving the workstation	The person has the attitude to leave unattended his/her device(s) logged in with his/her personal credential	PROXIMITY	USE	PROXIMITY	0.85	Low	0.77	High
unprotected_credential	Poor password management	The person has the attitude to use default or weak passwords or to not update them properly	PROXIMITY	OWN	PROXIMITY	0.85	High	0.44	High

CSV - Human Vulnerabilities

DRMP – Threat Analysis

- Calculating and prioritizing possible **attack paths** within a graph
- An **attack graph** represents possible ways via which an attacker can intrude into the target network by exploiting a set of vulnerabilities



POCT1
MedicalDevice

Linux - Android - 8

Type	CVE	Precondition	Postcondition
	CVE-2018-4846	USER	ROOT

Options

Visible Layers
☑ Network Layer
☑ Human Layer

Hide Networks

Graph Encoding
☑ Topology edges
☑ Attack Graph edges
☑ Nodes vulnerabilities

Queries

Options

Queries

Entities Type
● Nodes
○ Node Privileges

Sources

Targets
POCT1

The attack graph considers multidimensional paths (not only due to technical vulnerabilities but also related to humans and their access to the network)

DRMP – Risk Evaluation and Response Evaluation

- Based on the **multidimensional attack graph** and combined with
  - An **evaluation** of the business impact
  - Calculated from a precise **mapping of key business processes** vs infrastructural and human assets
  - Providing impact component for the risk computation

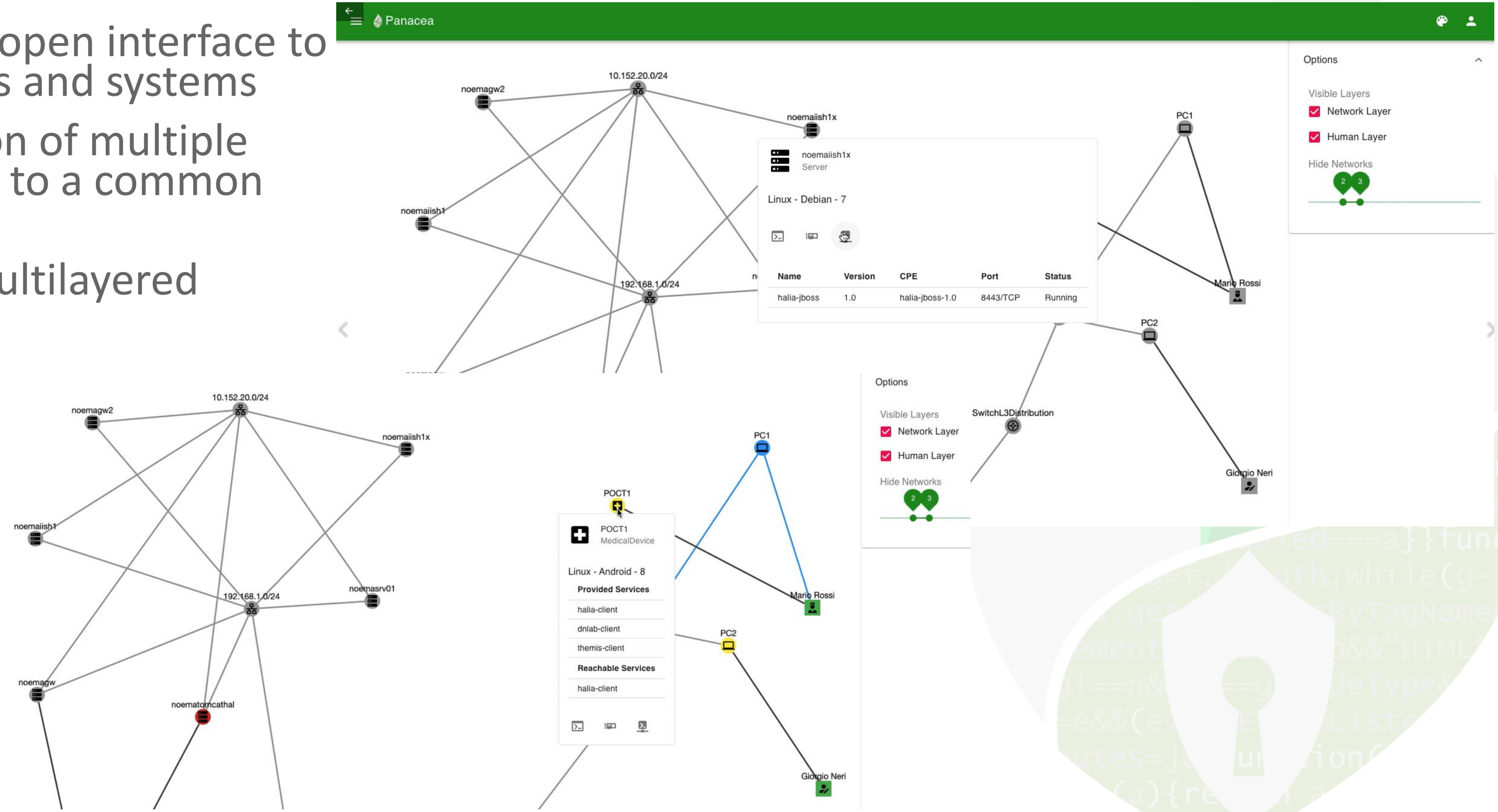
- Generating and **prioritizing** mitigation actions
- A list of **prioritized**, specific and **actionable** risk-mitigation actions is then generated, based on cost / impact / risk reduction trade-offs

Secure behaviours nudging
Resilience governance

Not only technical, but also governance, organizational and ‘human’ mitigation actions (nudging) to be considered by the response engine

DRMP – Visual Analytics Environment

- Flexible and open interface to COTS sensors and systems
- Normalization of multiple data sources to a common data model
- Advanced multilayered visualization



Panacea

Options

Visible Layers

☑ Network Layer

☑ Human Layer

Hide Networks

noemaiish1x
Server

Linux - Debian - 7

Name	Version	CPE	Port	Status
halia-jboss	1.0	halia-jboss-1.0	8443/TCP	Running

POCT1
MedicalDevice

Linux - Android - 8

Provided Services

halia-client

dnlab-client

themis-client

Reachable Services

halia-client

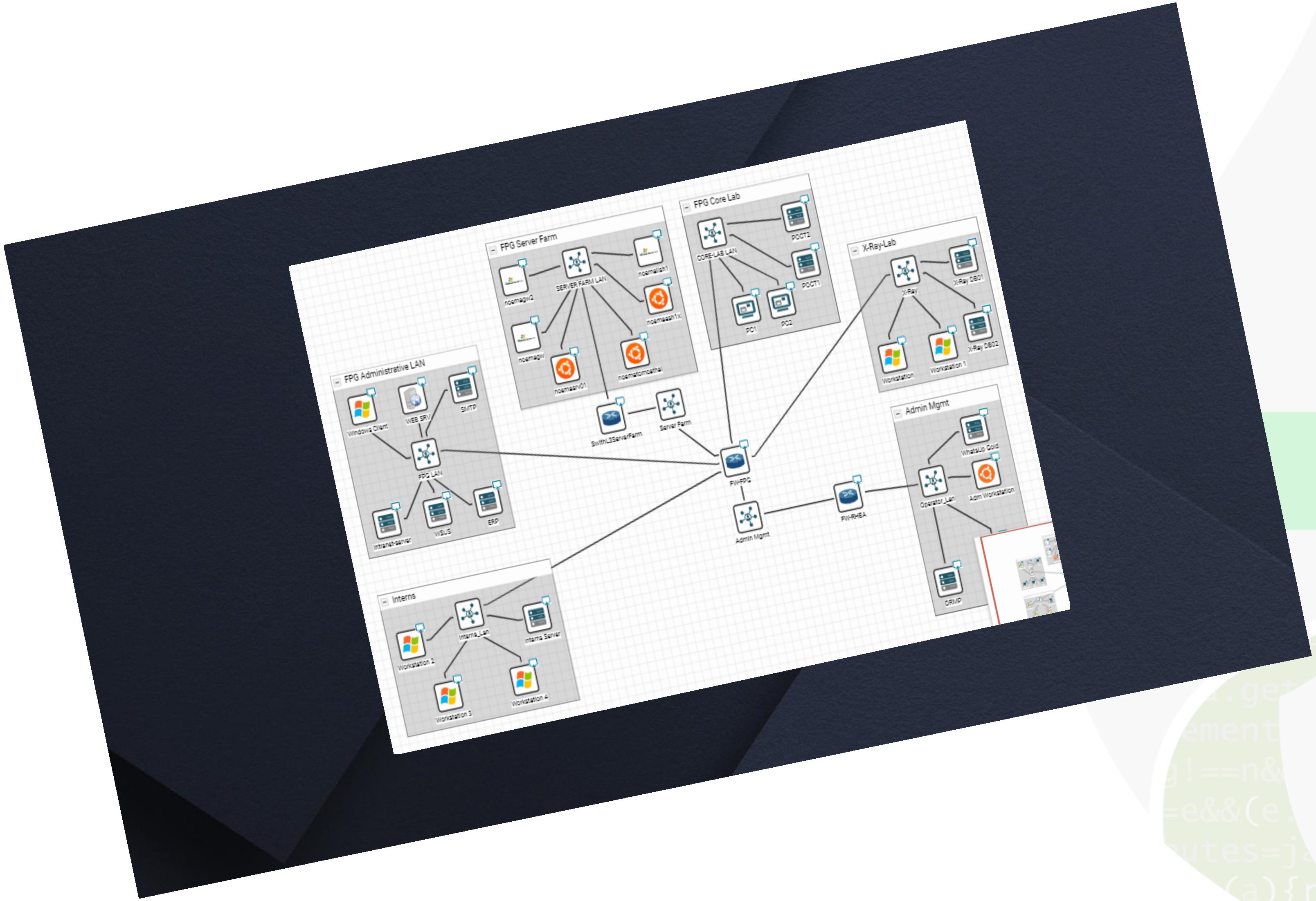
Emulation Environments

- As part of a research activity for the European Space Agency, RHEA developed a cyber range technology, CITEF
    - CITEF is used to create the PANACEA Emulation Environments, emulating identified networks within the End Users
    - PANACEA emulation environments will support (as from GA) DRMP R&D and validation activities

Emulation Environments

- Status
  - FPG Emulation Environment (linked to the User scenario 1-*FPG/LIS and connected Point of Care Testing*) is completed
    - Actually hosted in RHEA secure data centre in Redu (Belgium). This provides us a nice Healthcare cyber range we can reuse
    - HSE Emulation Environments are in definition phase

Emulation Environments - Demo


FPG Server Farm
noemagw2
SERVER FARM LAN
noemalish1
noemaash1x
noemagw
noemasrv01
noematomcathal
SwithL3ServerFarm
Server Farm
FPG Core Lab
CORE-LAB LAN
POCT2
POCT1
PC1
PC2
X-Ray-Lab
X-Ray
X-Ray DB01
X-Ray DB02
Workstation
Workstation 1
FPG Administrative LAN
Windows Client
WEB SRV
SMTP
FPG LAN
Intranet-server
WSUS
ERP
FW-FPG
Admin Mgmt
FW-RHEA
Admin Mgmt
WhatsUp Gold
Operator_Lan
Adm Workstation
DRMP
Interns
Interns_Lan
Interns Server
Workstation 2
Workstation 3
Workstation 4