Panacea

People-centric cybersecurity in healthcare

PANACEA: People-centric risk management for healthcare

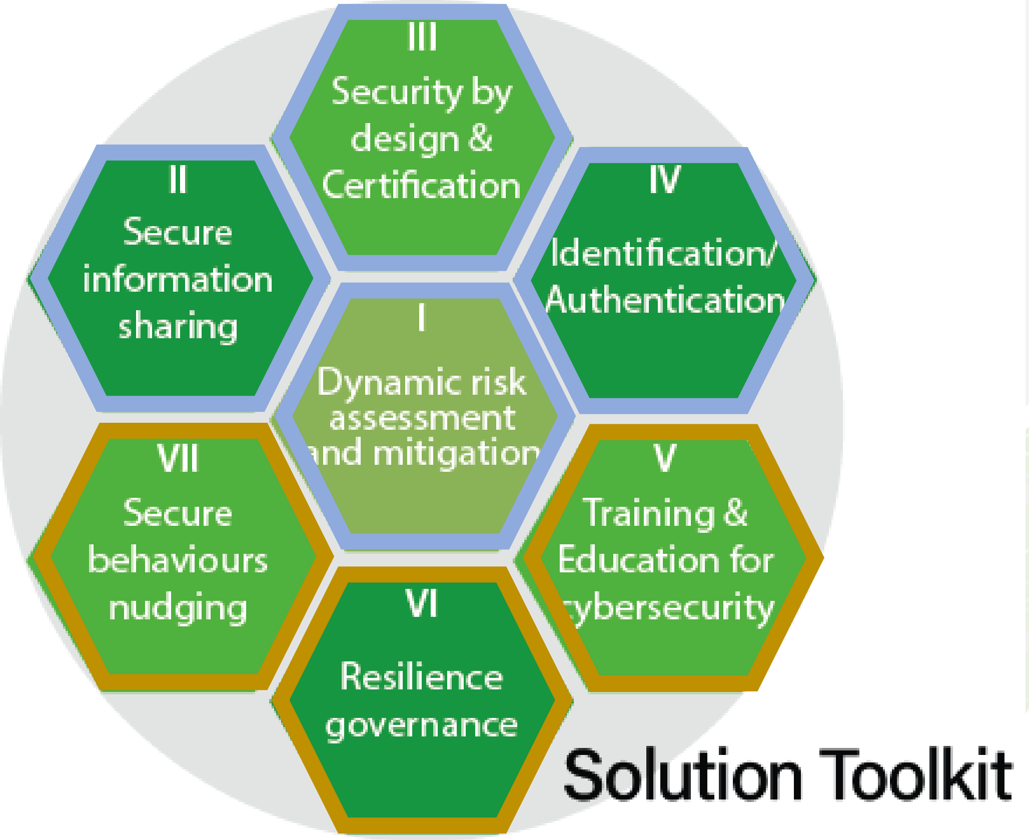
Fabrizio De Vecchis
RHEA

WEBINAR
23 November 2020

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

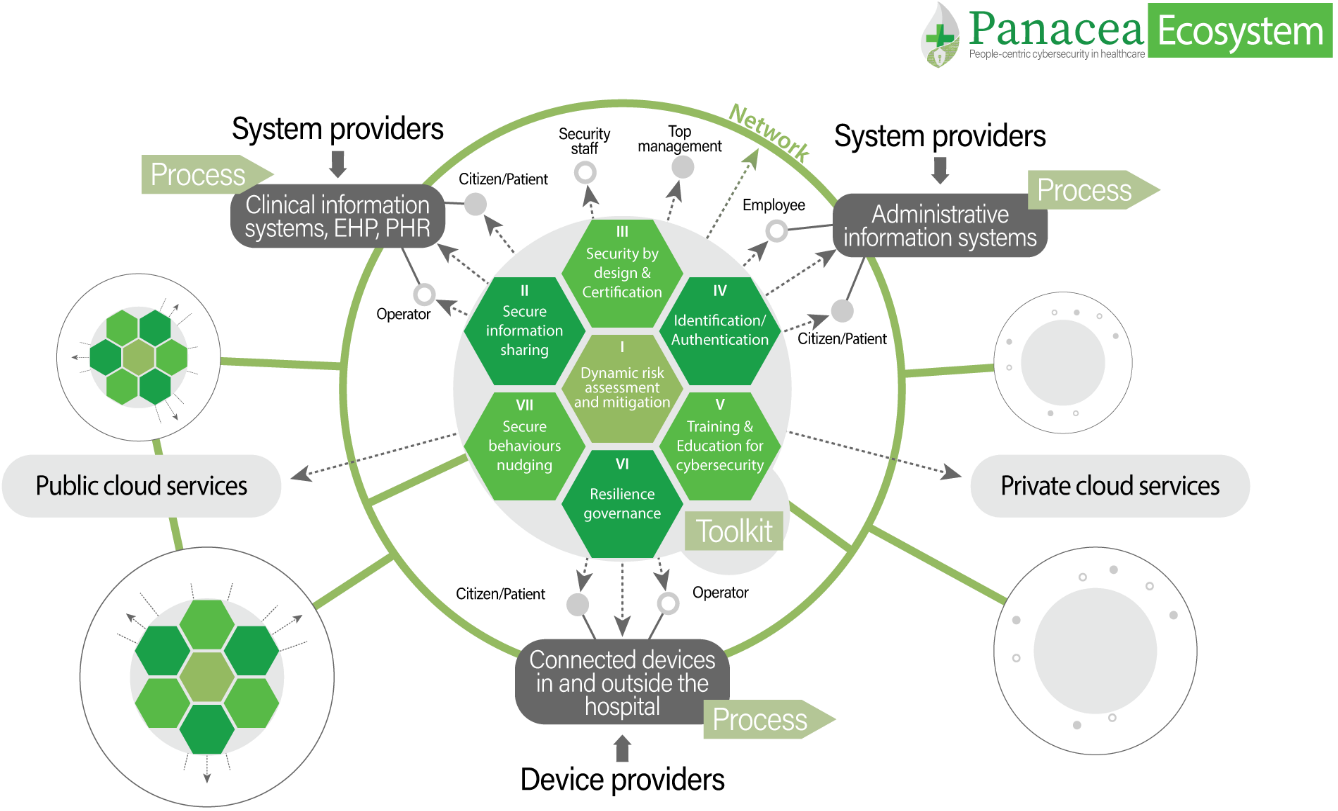
PANACEA Solution Toolkit

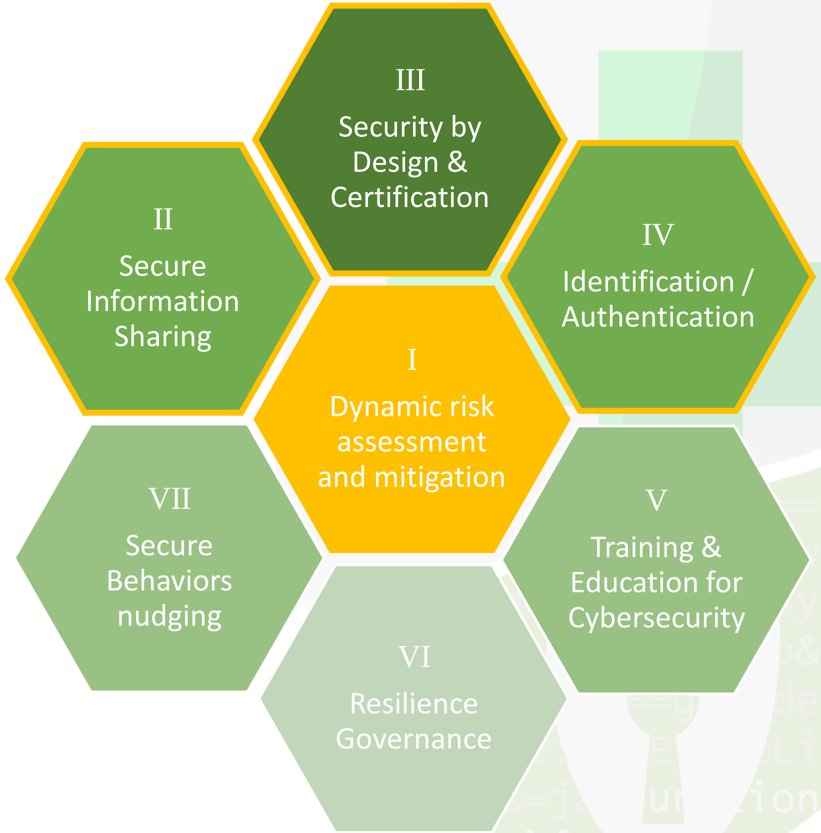
- The **PANACEA Toolkit** includes
  - **four technological tools** for
    - I-dynamic risk assessment & mitigation,
    - II-secure information sharing,
    - III-security-by-design & certification,
    - IV-identification & authentication
  - **three organisational tools** for
    - V-training & education,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

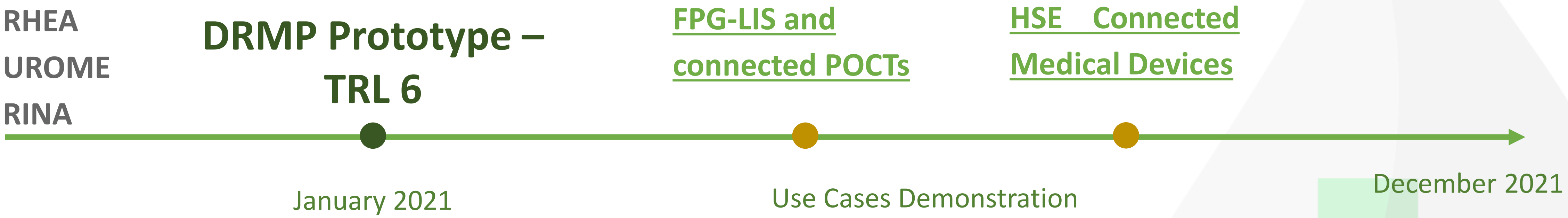
Solution Toolkit - DRMP

- **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
Citizen/Patient
Employee
Operator
System providers
Process
Administrative information systems
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

DRMP – Key Results



RHEA

UROME

RINA

DRMP Prototype – TRL 6

January 2021

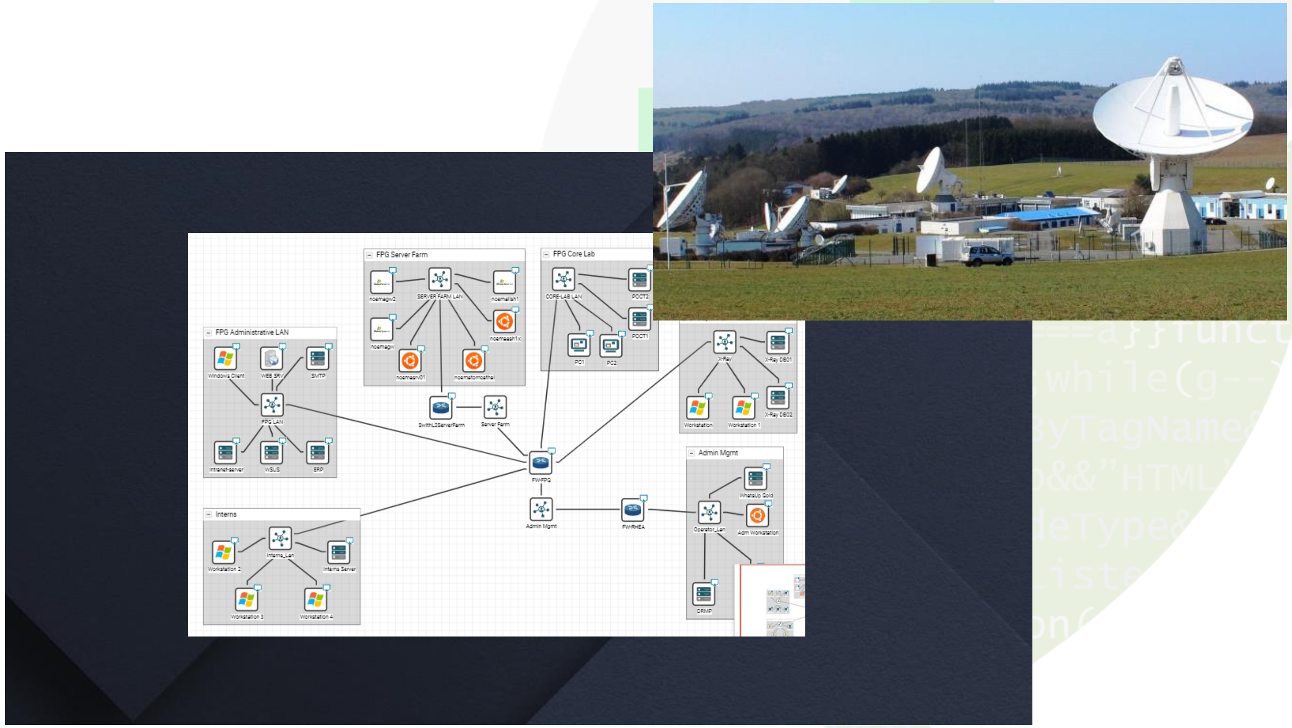
FPG-LIS and connected POCTs

HSE Connected Medical Devices

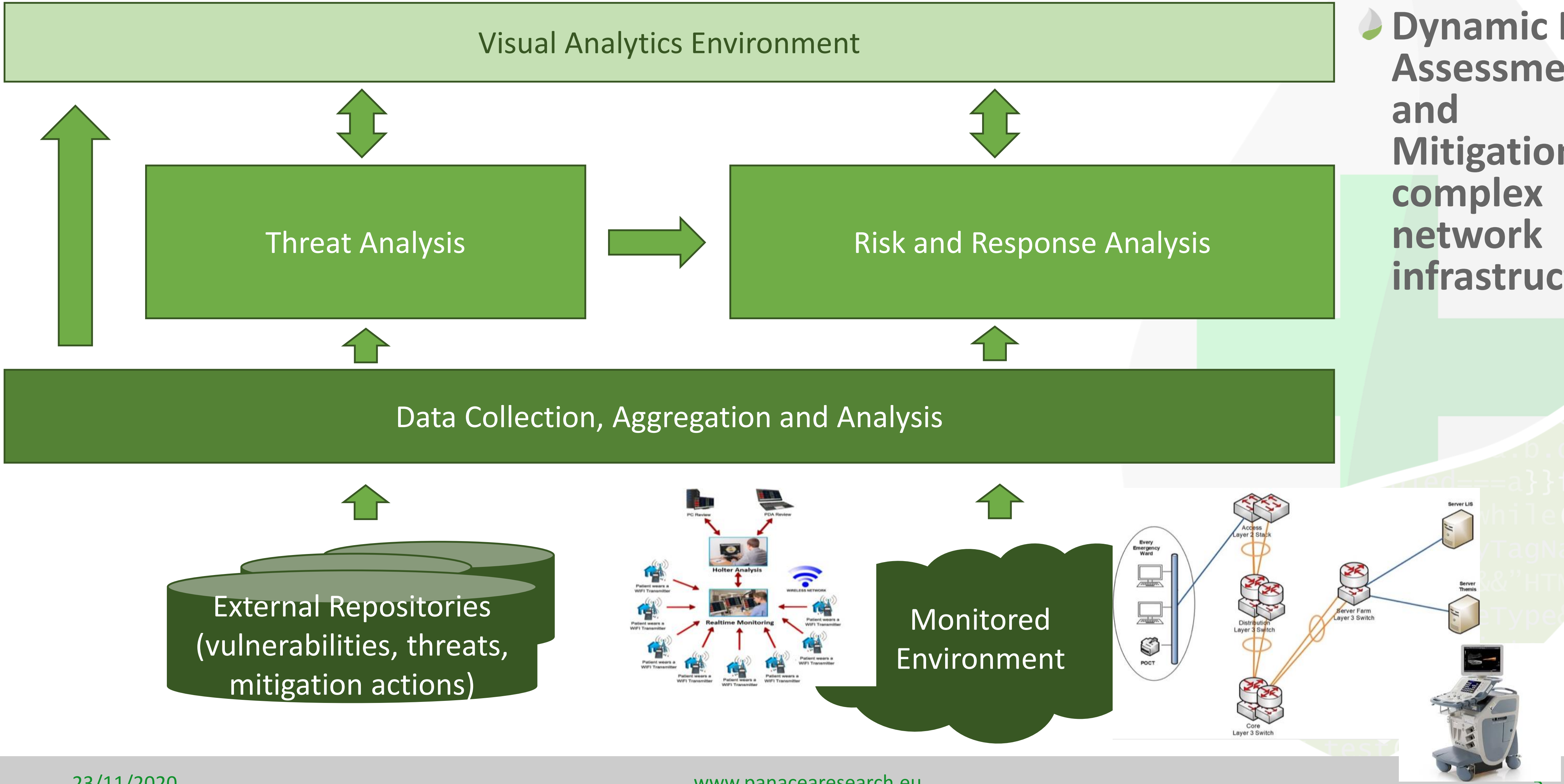
Use Cases Demonstration

December 2021

- FPG Emulation Environment (linked to the User scenario - *FPG/LIS and connected Point of Care Testing*) is completed
  - Actually hosted in RHEA secure data centre in Redu (Belgium).
  - HSE Emulation Environments are in definition phase



Dynamic Risk Management Platform (DRMP)



Visual Analytics Environment

Threat Analysis

Risk and Response Analysis

Data Collection, Aggregation and Analysis

External Repositories (vulnerabilities, threats, mitigation actions)

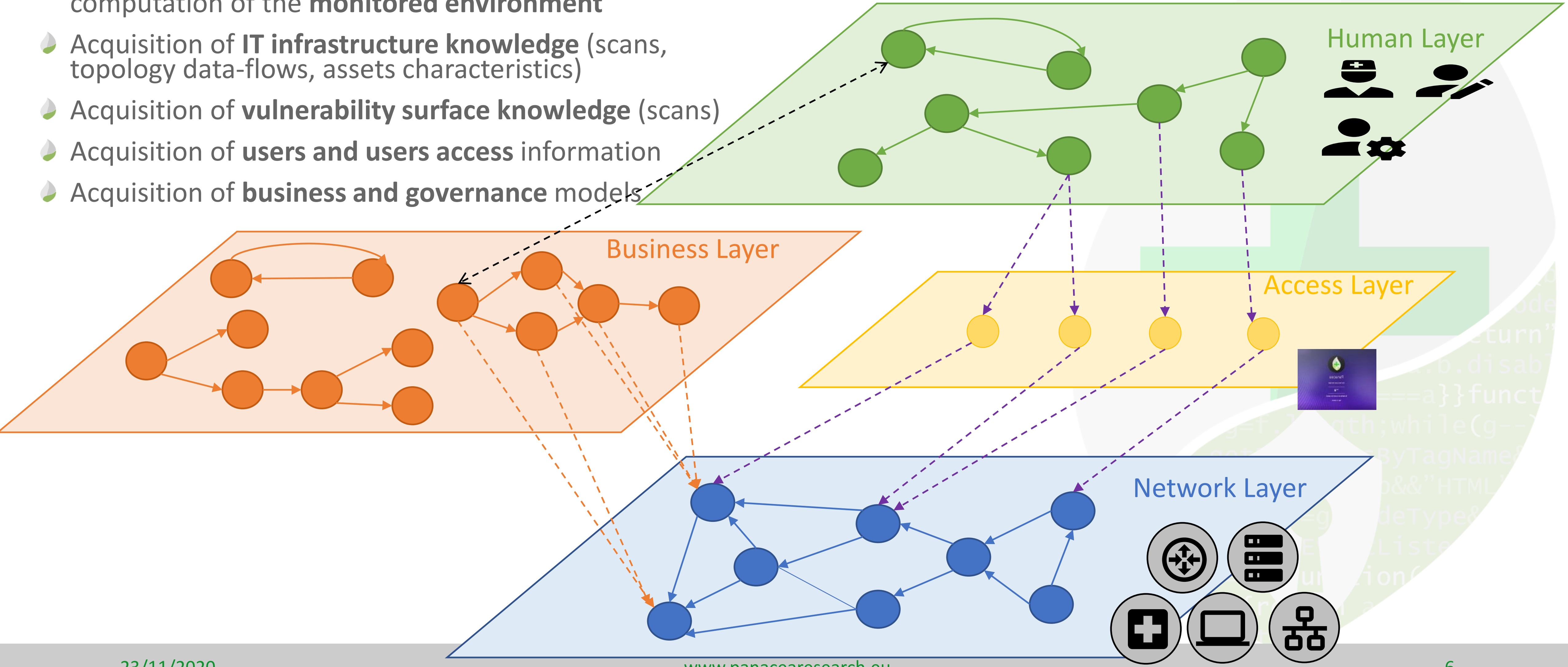
Monitored Environment

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
Every Emergency Ward
POCT
Access Layer 2 Stack
Distribution Layer 3 Switch
Core Layer 3 Switch
Server Farm Layer 3 Switch
Server LIS
Server Themis

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

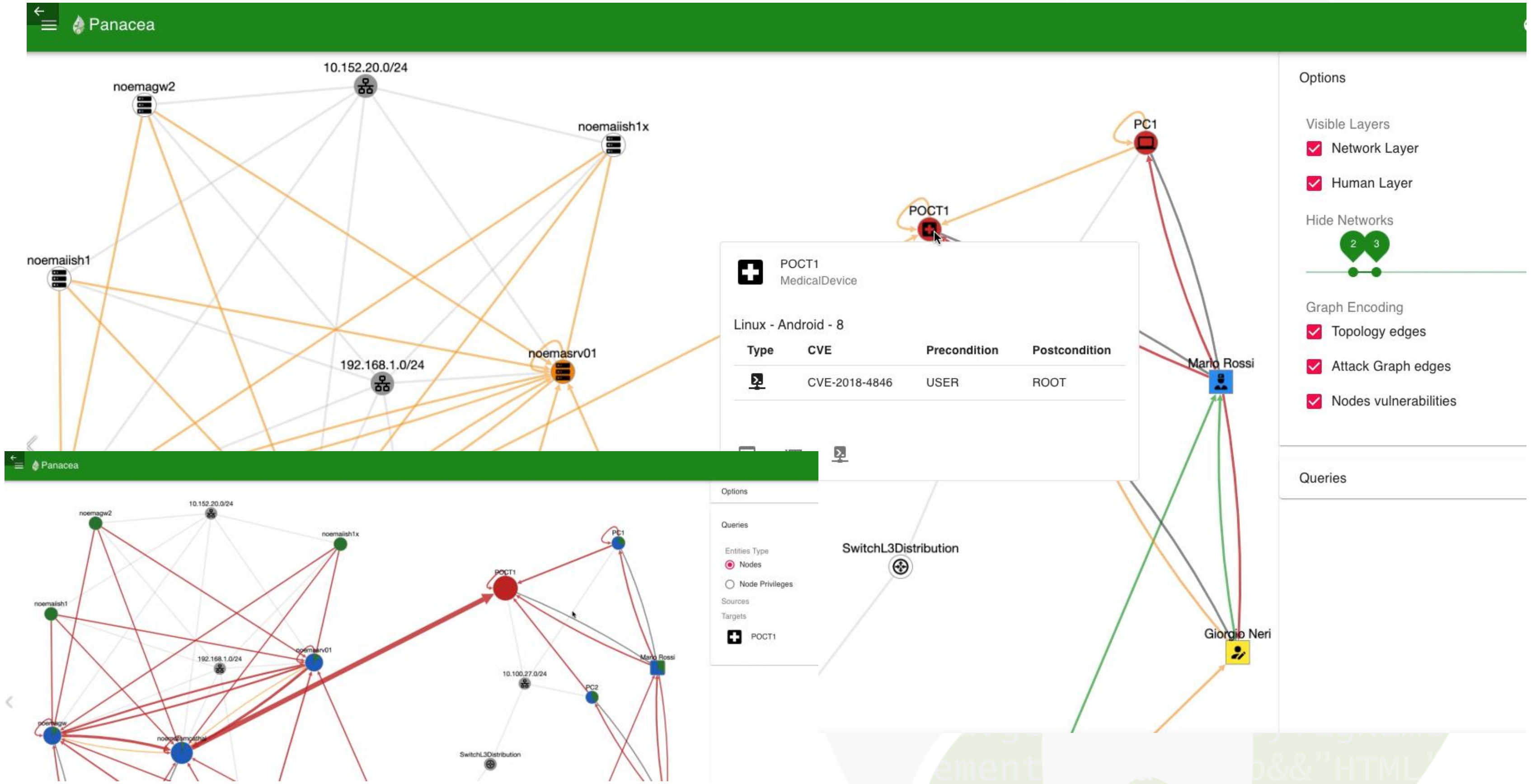
DRMP - Data Collection, Aggregation and Analysis

- **Multidimensional** data acquisition and reachability computation of the **monitored environment**
- Acquisition of **IT infrastructure knowledge** (scans, topology data-flows, assets characteristics)
- Acquisition of **vulnerability surface knowledge** (scans)
- Acquisition of **users and users access** information
- Acquisition of **business and governance** models



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

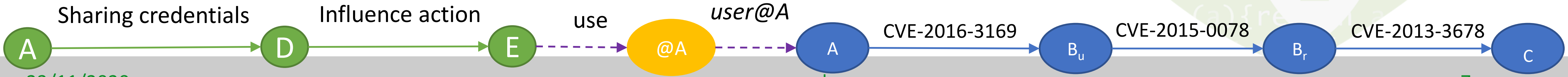


POCT1
MedicalDevice

Linux - Android - 8

Type	CVE	Precondition	Postcondition
	CVE-2018-4846	USER	ROOT

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

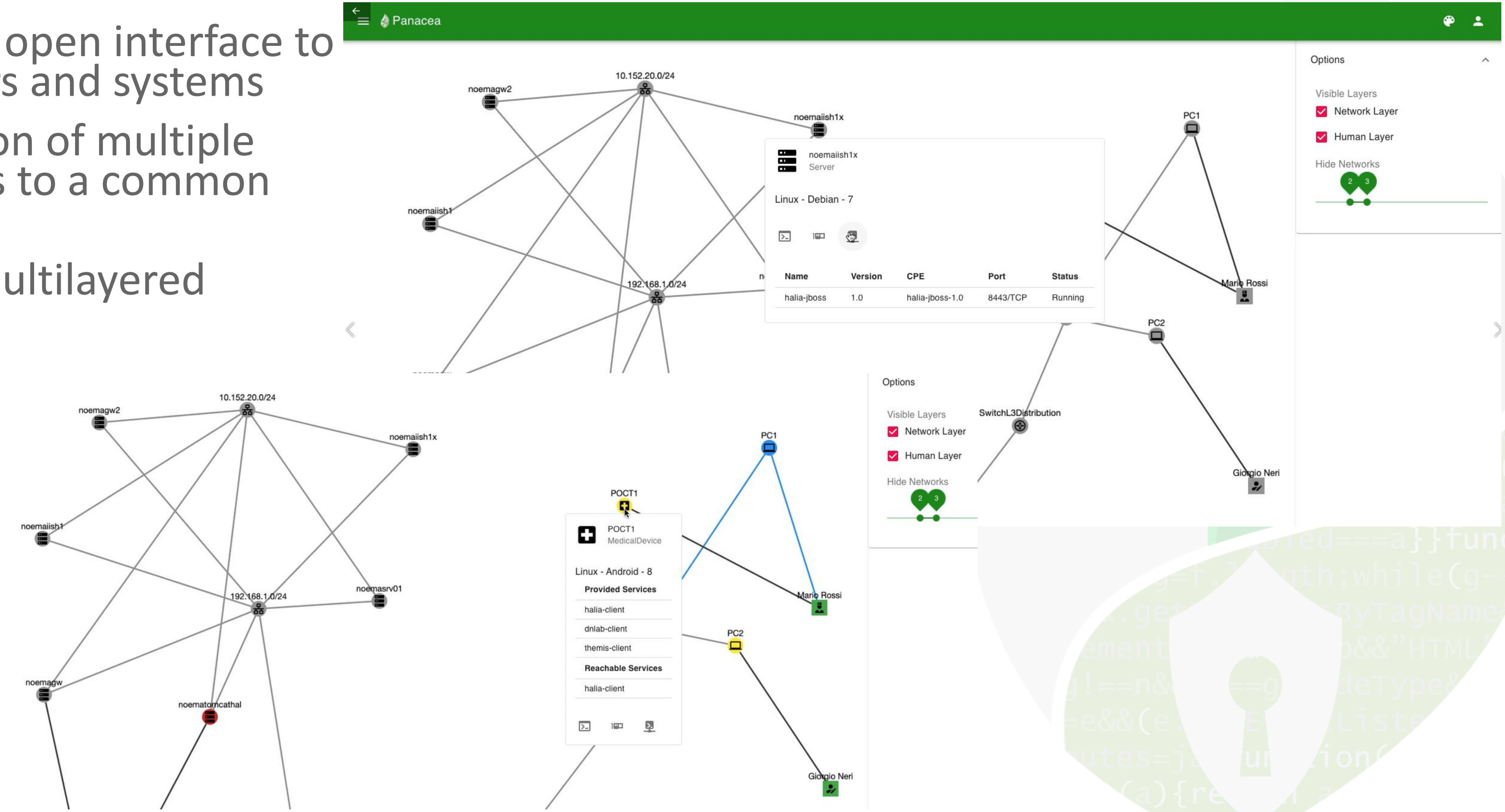
- Based on the **multidimensional attack graph** and combined with
  - An **evaluation** of the business impact
  - Calculated from a precise **mapping of key business processes** vs infrastructural and human assets
  - Providing impact component for the risk computation

- 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

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



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

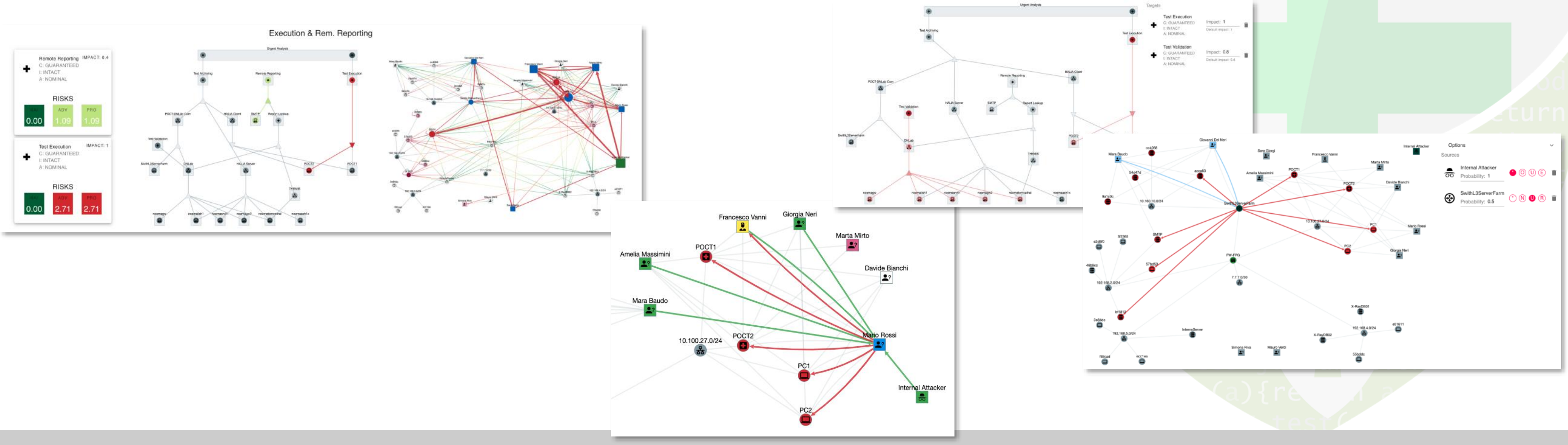
Reachable Services

halia-client

Dynamic Risk Management Platform (DRMP)

increase the cyber security resilience of the IT infrastructure of the HCCs

- new models able to rapidly capture and analyze the **multiple variables involved in a potential attack**, ranging from business, to human, to technical aspects
- **proactively and continuously protect a complex IT infrastructure** by quantitatively analyzing the current level of risk given a multi-dimensional threat analysis and the current business impact
- Semi-automatic identification of **response actions at both technical and non-technical level** to reduce organization risk
- support security operators with **increased situational awareness** and with **guided and interactive risk analysis**



Execution & Rem. Reporting

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

RISKS

NAI	ADV	PRO
0.00	1.09	1.09

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

RISKS

NAI	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
○ Ⓝ ● Ⓡ