SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Application Scenarios and Use Cases for SPHINX

Location: VUB-LSTS

CYBERSEC4HEALTH

Authors: Barbara Guerra and Marco Manso – EDGENEERING

Date: Brussels, July 10th, 2019

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

Outline

- **Application Scenarios**
- **Use Cases**
- **Pilots**

  Pilot 1: Securing Advanced Patient Care in Hospital and Homecare Environments

  Pilot 2: Cross-Border

  Pilot 3: Intra-Region

SPHINX Application Scenarios

5 Application Scenarios identified

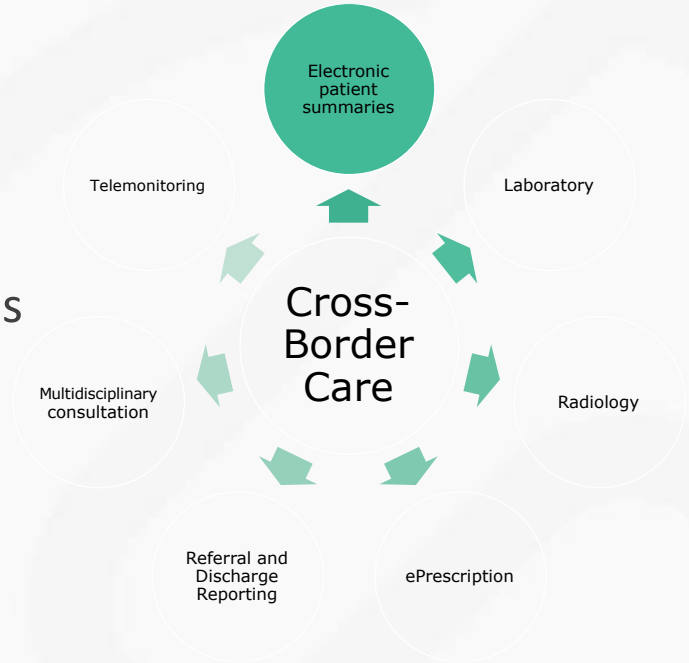
Digital Transformation in Healthcare

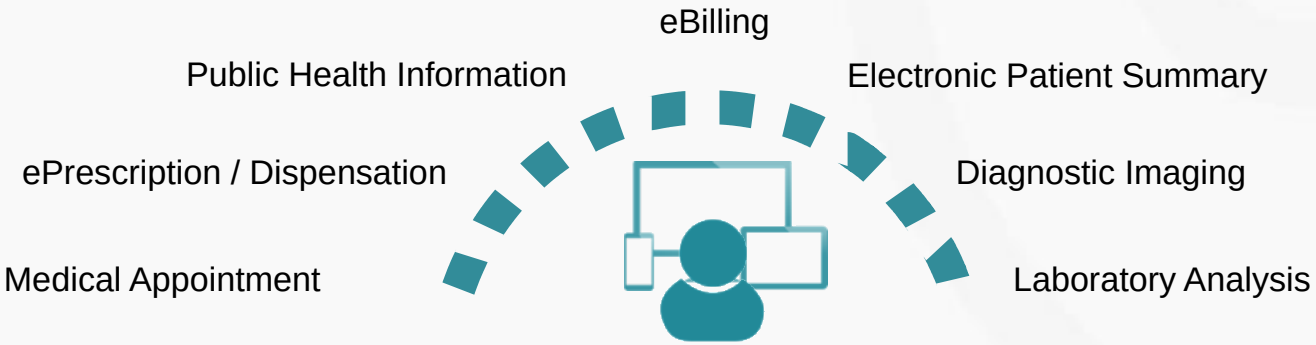
eHealth Services

mHealth and Remote Patient Monitoring Platforms

Sharing and Exchange of Healthcare Information

Cross-border Healthcare Service Delivery





SPHINX Application Scenarios

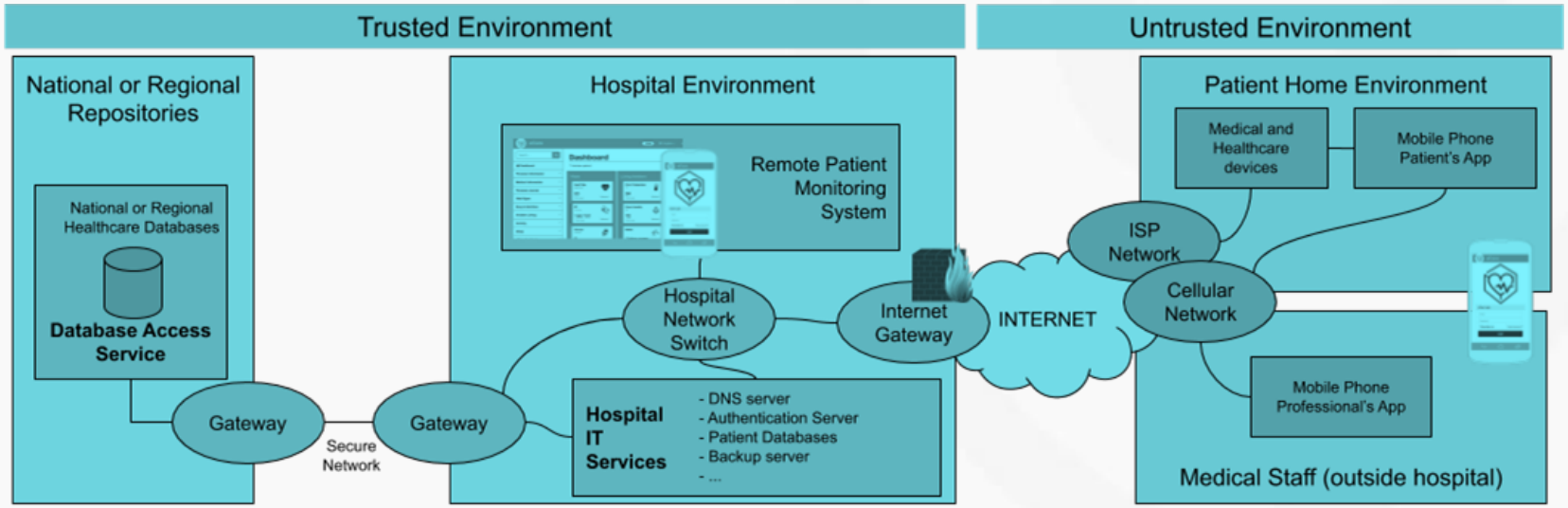
mHealth and Remote Patient Monitoring Platforms

Delivery of healthcare via remote access medical devices, IoT-based health devices (the Internet of Medical Things or IoMT) and mobile applications

Healthcare professionals can closely follow patients outside of the office, either through telehealth (video consultation) or remote patient monitoring

CHALLENGES

need to deal with: untrusted environments and devices; remote healthcare services (home care); integration of health professionals' and patients' BYOD devices in healthcare organisations' networks; users' authentication and profile management; availability, integrity and confidentiality of healthcare and patient data



SPHINX Use Cases

- **20+ use cases proposed (work in progress)**
- **Each contains:**

Scope: identification of the applicable scenario

Attack: identification of the type of threat, the threat actor(s) and the attack vector(s)

Vulnerability and exploitation

Critical healthcare assets

Description

Attack impact: outline of the negative effects inflicted by the attack, considering the healthcare IT ecosystem, the healthcare organisation and key stakeholders;

SPHINX's role and added value benefits

SPHINX Use Cases

1. Attacking Obsolete Operating Systems
2. Hijacking Access to National Healthcare Databases
3. Rootkit Malware Attack in a Cancer Treatment Institute
4. Healthcare Data Theft
5. Tampering with Medical Devices
6. Ransomware Attack to Healthcare Data
7. Distributed Denial-of-Service Attack in Regional Hospital
8. Compromising Health Services through Cryptocurrency Mining
9. Compromised BYOD Enables Stealing of Patient Data
10. Taking Control of a Connected Medical Device
11. Intrusion in the Clinical Centre's Wireless Network
12. Hacking Health IT Systems
13. Exploiting Remote Patient Monitoring Services
14. Zero Day Attack to eHealth Services
15. Theft of Hospital Equipment
16. Failure of Hospital IT Infrastructure in Heavy Storm
17. Misconfiguration of IT Equipment Causing QoS Disruption
18. Transfer of Medical Devices Between Healthcare Providers
19. Cross-border Healthcare Data Exchange
20. Digital Identity Theft of a Medical Doctor
21. Illicit Rewriting of Patients' Medication Prescription
22. Exploiting Medical Equipment to Steal Exams Results

Use Case: Attacking Obsolete Operating Systems

Use Case: Attacking Obsolete Operating Systems	
Scope	
Application Scenario	Digital Transformation in Healthcare
Attack	
Threat Type	Malicious action – Social engineering and Malware; System failure – Legacy and obsolete systems
Threat Actor(s)	Remote attackers – Opportunistic
Attack Vector(s)	Interaction with users (social engineering)
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	User with privileged access Legacy and obsolete IT system
Critical Healthcare Assets	
Affected Asset(s)	Healthcare information systems IT and networking equipment
Criticality of Affected Asset(s)	Highly critical

Use Case: Attacking Obsolete Operating Systems

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Cond.	A hospital employee uses a virtual machine with an obsolete operating system.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including operating systems that are obsolete, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The employee occasionally surfs the Internet using the computer's virtual machine.	
Attack Phase	The employee accidentally downloads and executes a file infected with malware. The malware propagates to several assets in the hospital's network. The malware creates botnets, congests the local network and servers and locks out user accounts. Hospital's medical, nursing and administrative staff are forced to switch to hardcopy-based operations (paper operations) in order to perform their work activities and deliver care services.	SPHINX detects the access to flagged websites, web traffic and suspicious content (e.g., malicious files) and blocks access to it. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX recognises the machine's erratic behaviour (e.g., excessive CPU load and traffic), the malicious (botnet) behaviour and traffic (connection attempts to C&C servers, traffic to unusual TCP/UDP ports) and isolates the infected assets from the rest of the network, denying the malware access to additional resources and effectively countering malware propagation attempts. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department has to proceed with a clean installation of computers (resorting to backup systems to partially recover hospital records).	SPHINX collects relevant attack-related data, including compromised components (e.g., OS, files, protocols), attack patterns, IP packets and remote addresses (IP of the C&C server) and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Use Case: Exploiting Medical Equipment to Steal Exams Results

Use Case: Exploiting Medical Equipment to Steal Exams Results	
Scope	
Application Scenario	Digital Transformation in Healthcare
Attack	
Threat Type	Malicious action – Medical device tampering
Threat Actor(s)	Remote attacker – Cyber-criminal
Attack Vector(s)	Wireless communication with IT assets
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	Connected medical equipment
Critical Healthcare Assets	
Affected Asset(s)	Networked medical devices; Healthcare data
Criticality of Affected Asset(s)	Highly critical

Use Case: Exploiting Medical Equipment to Steal Exams Results

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A medical equipment manufacturer made a large investment in introducing connectivity to its new device's portfolio. The manufacturer used the openSSL (version 1.0.1) to implement secure TLS/SSL connections, however was unaware of the Heartbleed bug. The manufacturer is selling its devices to customers.	SPHINX performs a cybersecurity certification of the medical equipment in manufacturer environment (before being deployed in customer premises). The manufacturer receives a report identifies the measures to be taken to remove the cyber vulnerabilities detected in order to establish a secure device. Only when the medical device equipment receives the SPHINX approval of full security compliance, is it put to market.
Pre-Attack Phase	Posing as a visitor to a patient admitted to the clinic, a cyber-criminal connects to the clinic's WiFi network and finds the medical equipment using the openSSL version 1.0.1.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and reports to the IT department the system's major vulnerabilities.
Attack Phase	The attacker uses a Heartbleed exploit to retrieve secret keys used for the X.509 certificates, user names and passwords and exam result documents (i.e., sensitive data collected by the device like the patients' exams results). The attacker contacts the clinic to demand a ransom in bitcoin to return the stolen patient data.	SPHINX detects the vulnerability in the compromised equipment and transfers them to an isolated network environment for further inspection. SPHINX generates an alert of the suspicious activity (remote access to device data from an unknown computer) to warn the IT department and provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department identifies the compromised medical equipment, disconnects them from the network and requests the manufacturer to fix the vulnerability. Once fixed by the manufacturer, the IT department reconnects the device to the network.	SPHINX collects relevant attack-related data, including the compromised network components. The IT department decides to share this information with the manufacturer, allowing the latter to learn about the equipment's vulnerabilities. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attacks.

Scenarios and Use Cases Matrix

Use Cases	UC01	UC02	UC03	UC04	UC05	UC06	UC07	UC08	UC09	UC10	UC11	UC12	UC13
Application Scenario													
Digital Transformation in Healthcare	•		•			•		•				•	
eHealth Services				•									
mHealth and Remote Patient Monitoring Platforms					•		•		•	•	•		•
Sharing and Exchange of Healthcare Information		•											
Cross-border Healthcare Service Delivery													
Attack													
Malicious actions: Malware	•		•	•	•			•	•				•
Malicious actions: Hijacking		•									•		
Malicious actions: Medical device tampering					•					•			
Malicious actions: Ransomware						•							
Malicious actions: Distributed Denial of Service							•						
Malicious actions: Social Engineering	•			•		•				•	•		
Human error									•			•	
System failure	•												
Attack Vectors													
Physical interaction with IT assets								•					
Wired communication with IT assets			•	•	•	•							
Wireless communication with IT assets		•					•				•	•	•
Interaction with users	•		•	•	•	•			•			•	
Attack Actors													
Remote: Attackers: Government Sponsored										•			
Remote: Attackers: Organised Crime						•							
Remote: Attackers: Cyber Terrorists			•										
Remote: Attackers: Hacktivists				•									
Remote: Attackers: Opportunistic	•						•		•				•
Insider threats					•			•					
Malicious external users		•									•	•	
Affected Assets													
Healthcare Information Systems	•			•		•	•					•	
Healthcare data repositories			•			•						•	
Identification System			•						•			•	
Networked medical devices					•					•		•	
Mobile user devices									•			•	
IT and networking equipment	•	•	•				•	•			•	•	
Healthcare data			•	•		•			•	•		•	•
Impact													
Loss of availability	•	•			•	•	•	•			•	•	
Data Integrity Violation			•		•					•		•	•
Data Confidentiality Violation			•	•					•	•		•	

SPHINX Pilots

3 Pilots planned in SPHINX

Securing Advanced Patient Care in Hospital and Homecare Environments

HESE + EDGE

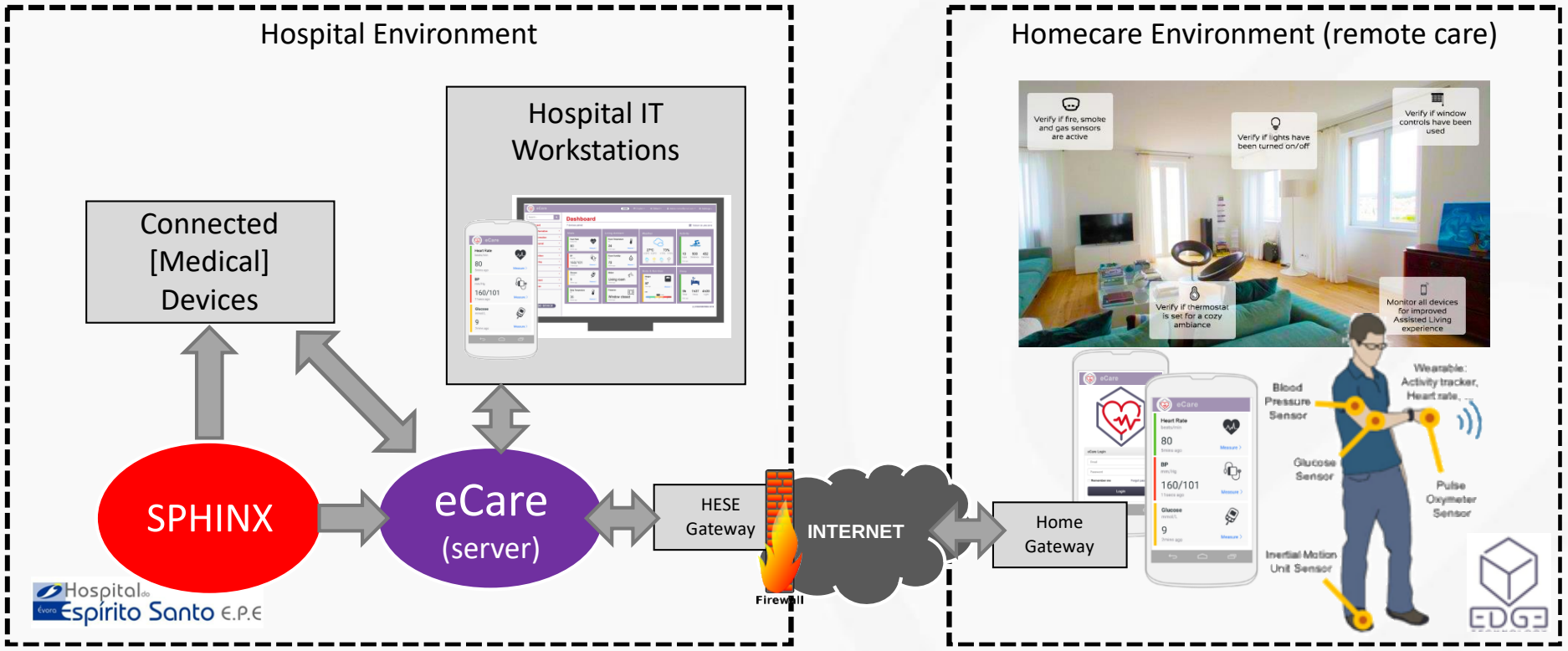
Cross-border Romania-Greece

POLARIS (Private Clinic) + DYPE5 (Regional Authority)

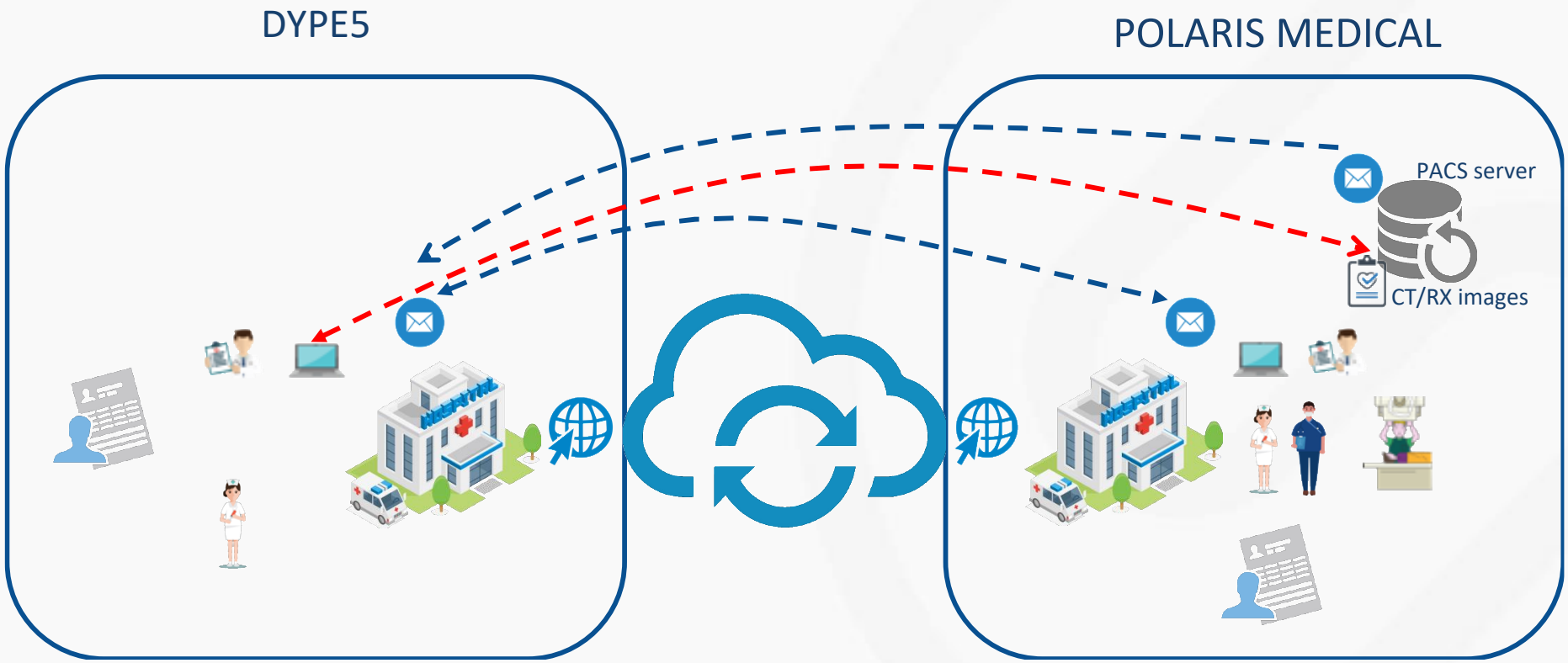
Intra-region in Greece

Hospital Volos + Hospital Larissa (part of DYPE5)

Pilot 1: Securing Advanced Patient Care in Hospital and Homecare Environments

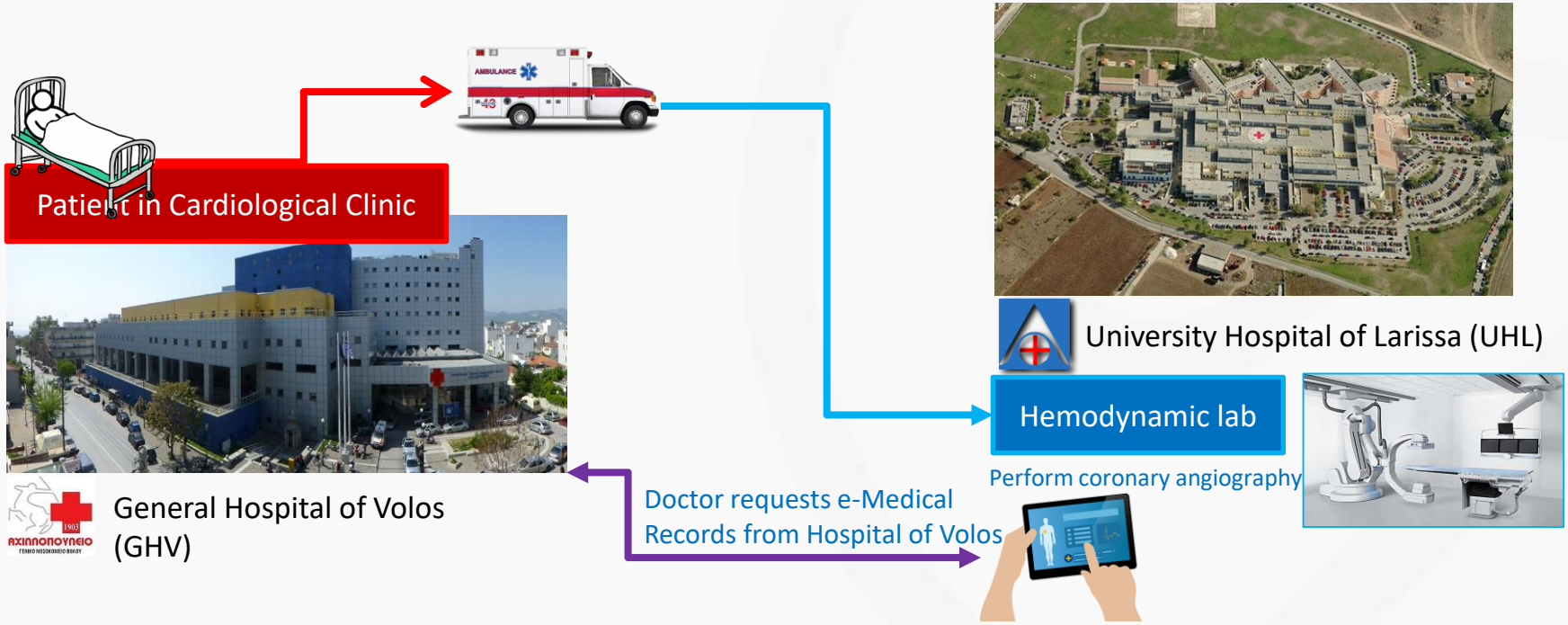


Pilot 2: Cross-Border



Pilot 3: Intra-Region

- Patient Transfer from General Hospital of Volos to University Hospital of Larissa within the region of 5th Regional Health Authority (DYPE5)



References and Sources

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. September 2012. Version 3.1, Revision 4.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components. September 2012. Version 3.1, Revision 4.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components. September 2012. Version 3.1, Revision 4.
4. ENISA Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures. European Union Agency for Network and Information Security. November 2016.
5. ENISA Security and Resilience in eHealth - Security Challenges and Risks. European Union Agency for Network and Information Security. 2015
6. ENISA Reference Incident Classification Taxonomy - Task Force Status and Way Forward. European Union Agency for Network and Information Security. January 2018.
7. https://github.com/MISP/misp-taxonomies.
8. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/ontology_taxonomies.
9. https://www.csoonline.com/article/3203804/know-your-enemy-understanding-threat-actors.html.
10. https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/threats-attacks-and-vulnerabilities-in-security/how-to-explain-threat-actor-types-and-attributes/#gref.
11. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.
12. Data Breach Investigations Report. Verizon Enterprise. 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.
13. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. Ponemon Institute. 2016. https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.
14. Accenture 2018 Healthcare Workforce Survey on Cybersecurity. Accenture. YouTube. 2018. https://www.youtube.com/watch?v=1WI_o7VQQxI.
15. Gavin O'Brien et. al. Securing Electronic Health Records on Mobile Devices. National Institute of Standards and Technology. July 2018. https://doi.org/10.6028/NIST.SP.1800-1.
16. The Internet of Things 2019. Peter Newman. Business Insider Intelligence. January 2019.
17. Unlocking the potential of the Internet of Things. James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. McKinsey Global Institute. June 2015.
18. 19 million will use remote patient monitoring by 2018. MEDCITY News. http://medcitynews.com/2014/06/biggest-market-remote-patient-monitoring/.
19. Conficker Working Group. Lessons Learned. June 2010. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

Presenter Name: Marco Manso
Organisation: EDGENEERING
Email: marco@edgeneering.eu

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