# ECHO Federated Cyber Range as a Tool for Validating SHAPES Services

**Jyri Rajamäki and Harri Ruoslahti**
**Laurea University of Applied Sciences, Espoo, Finland**
jyri.rajamaki@laurea.fi
harri.ruoslahti@laurea.fi

DOI: 10.34190/EWS.21.076

**Abstract:** ECHO is a cybersecurity pilot project under the H2020 Program. The ECHO Federated Cyber Range (E-FCR) provides enabling technology supporting ECHO Network operations, ensuring a safe and reliable multi-sector simulation environment in which to ensure viable delivery of identified technology roadmaps, as well as, hands-on cyber-skills development involving realistic sector specific or multi-sector simulations. A cyber range leverages cloud technologies to provide a virtualized environment in which realistic cyber scenarios can be instantiated. The eHealth platform by project SHAPES will rely on services and products provided by vendors. Operability and usability of the platform requires reliable, uninterrupted and well-managed actions from the systems utilized to run services of the eHealth platform. The SHAPES platform operates in the cyber domain and the taxonomy of cyber-risks vary from actions of people due lack of cybersecurity awareness to technology failures. Moreover, threats from malicious external sources might exploit vulnerabilities of SHAPES assets and therefore cause damage. Predefined security validation procedures facilitate to create a baseline for services and their desired level of security. This work-in-progress paper explores how to apply E-FCR during eHealth-services validation processes. The paper profits two Horizon-2020 projects: The ECHO cybersecurity project demonstrating how to utilize E-FCR in the healthcare domain; and the SHAPES healthcare project that needs a cybersecurity validation processes for services incorporated into the SHAPES platform.

**Keywords:** ECHO project, SHAPES project, federated cyber range, security validation

## 1. Introduction

Data breaches in the healthcare sector are occurring at unprecedented rates, and the causes of these breaches have not delineated very well (McLeod & Dolezel, 2018), so protecting the cyber environment of healthcare systems and operators is important in protecting society and its critical infrastructure.

Project *Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES)* gathers stakeholders from across Europe to create, deploy and pilot at large-scale an EU-standardized open platform integrating a broad range of technological, organizational, clinical, educational and societal solutions. The aim is to enable ageing Europeans to remain healthy, active and productive, while maintaining a high quality of life and sense of wellbeing for the longest time possible (European Commission, 2019). *European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)* is one of four European pilot projects, which together aim to establish and operate a European network of cybersecurity excellence. During its four-year life span, ECHO will develop and deliver an organized and coordinated, effective and efficient multi-sector collaboration based approach that helps strengthen the proactive cyber defences of the European Union (Pappalardo et al., 2020).

In January 2021, the ECHO project started working on the Demonstration Cases that are key to validate ECHO technology roadmaps and their combination. The SHAPES project needs a cybersecurity validation processes for services incorporated into the SHAPES platform. This work-in-progress paper explores possibilities to apply ECHO's Federated Cyber Range (E-FCR) to validate eHealth-services. This paper is organized as follows: Section 2 deals with cybersecurity of eHealth platforms. Section 3 outlines security validation requirements for eHealth services. Section 4 presents ECHO's work in the healthcare sector and E-FCR. Section 5 concludes the paper and suggests possibilities for future work.

## 2. eHealth platform

ENISA, the European Union Agency for Cybersecurity (2020) has listed various threats to hospitals including system, device, software or network component failures, human errors, and malicious actions such as denial of service or web application attacks. Supply chain failures, cloud service provider failures especially, are an important threat source (ENISA, 2020). The SHAPES eHealth platform combines in-formation technology and communication components to support the well-being of elderly people, mainly technologies and information or primarily clinical and medical purposes, while academic study and decision-making can use secondary information.

ENISA (2015) identifies critical platform assets: Health information systems; Databases; Authentication server; Laboratory and radiology information systems; Electronic health record components and service; ePrescription services.

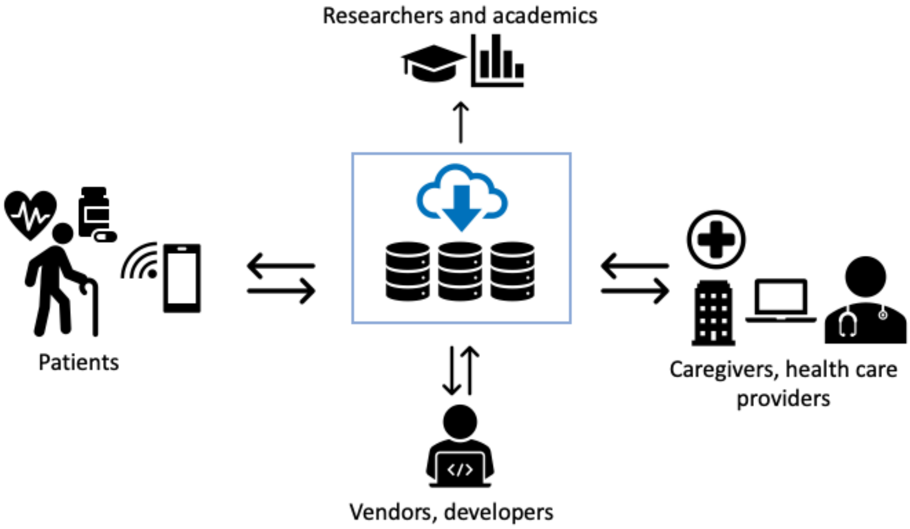

**Figure 1:** eHealth ecosystem

Figure 1 above presents a simplified illustration of the eHealth platform. Health data is centralized to the SHAPES Secure Cloud that would act as a hub between ecosystem stakeholders, store patient data, and allow personalised services for patients. Aggregated big data from patients would be used secondarily after modifications to ensure anonymous origin of data/information.

The eHealth ecosystem includes the critical assets (ENISA, 2015): healthcare providers have components of network devices, patient and caregiver use web applications to access information stored in data-bases and both authenticate themselves to services through an identity management system. Patients have devices to save daily results of exercise and blood-pressure for later evaluation.

Baselines for information security policies e.g. acceptable use policy for services and general security awareness requirements (ENISA, 2020) should be addressed by SHAPES so that ecosystem stakeholders understand the importance of safeguarding sensitive information and what risks are related to mishandling information. Figure 2 presents how PCI Security Standards Council (2014) relates risk levels, roles with depth of security awareness training, emphasising the importance of awareness training as part of overall risk management activities.

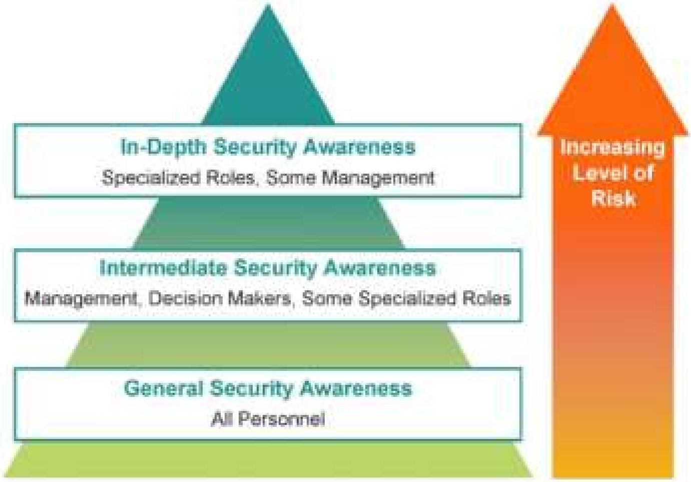
In-Depth Security Awareness
Specialized Roles, Some Management
Intermediate Security Awareness
Management, Decision Makers, Some Specialized Roles
General Security Awareness
All Personnel
Increasing Level of Risk

**Figure 2:** Security awareness and level of risk (PCI Security Standards Council, 2014)

## 3. Requirements for validating eHealth services

Information and data protection requirements for social and healthcare procurement by Finnish National Cyber Security Centre (NCSC-FI) are presented in themes under headings. These requirements are directional but not definite for every procurement (Traficom, 2019). The original file with requirements can be accessed from NCSC-FI web page. The following requirements may help mitigate risks against SHAPES assets. ENISA (2020) has similar guidelines for procurements in hospitals. ENISA guidelines have been separated to three phases: plan, source and manage in addition to general good IT practices. All phases encourage hospitals to embrace good practices for cybersecurity. Table 1 presents similarities between these two publications:

**Table 1:** Similarities in NCSC-FI requirements and ENISA guidelines

| Phases in ENISA's guidelines | ENISA | NCSC-FI |
|---|---|---|
| General practices | Involve IT department in procurement<br>Vulnerability management<br>Policy for hardware and software<br>Secure wireless communication<br>Establish testing policies<br>Establish Business Continuity Plans<br>Consider interoperability issues<br>Allow auditing and logging<br>Use encryption | Wireless systems<br>Incident support<br>Secure architecture<br>Logging<br>Certificate and key management<br>Interface security<br>On-premises installations<br>Inform personnel |
| Plan phase | Conduct risk assessment<br>Plan requirements in advance<br>Identify threats<br>Segregate network<br>Establish eligibility criteria for suppliers<br>Create dedicated RfP for cloud | Risk management<br>Segmentation & data flows<br>Data protection & safekeeping<br>3rd party software<br>Security control |
| Source phase | Require certification<br>Conduct DPIA<br>Address legacy systems<br>Provide cybersecurity training<br>Develop IRP<br>Involve supplier in incident management<br>Organise maintenance operations<br>Secure remote access<br>Require patching | Security patch management<br>System administration<br>Personal data protection<br>On-premises installations<br>Incident support<br>Security control<br>System privacy<br>Personnel security contracts |
| Manage phase | Raise cybersecurity awareness<br>Perform asset inventory and configuration<br>Dedicated access control mechanisms<br>Schedule penetration testing frequently or after modifications in the architecture/system | Security testing<br>System & security monitoring<br>User accounts & authentication<br>User rights & session management<br>Change management<br>3rd party software<br>Inform personnel<br>Organisational and personnel changes<br>System and information disposal |

## 4. ECHO Federated Cyber Range (E-FCR)

ECHO develops cybersecurity technology roadmaps based on analysis of current and emerging cybersecurity challenges and associated technologies. These roadmaps may serve as foundations for novel industrial capabilities, and in developing new and innovative technologies to address the cybersecurity challenges of Europe. Research and development of early ECHO prototypes will target high-priority opportunities specified in the six ECHO roadmaps, one of which is the E-FCR (Kirkov et al., 2020).

E-FCR combines capabilities of several independent interconnected cyber-ranges, and can help simulate inter-sector scenarios that include complex realities and inter-sector dependencies (Kirkov et al., 2020). The healthcare sector, which offers life-critical services, is increasingly adopting new technologies, which while they intend to improve treatment and care, they may also be vulnerable to cyber threats (McLeod & Dolezel, 2018). In the health sector cyber-incidents not only threaten the security of medical systems and information, but patients' lives. New medical technology adds value to healthcare only when it is (cyber) secure (Pappalardo et al., 2020).

ECHO recommends reducing complexity in healthcare systems, raising awareness, and specifying cybersecurity skills and training curricula for all levels of healthcare staff. Hospital and organizations should budget for increased and cybersecurity risk assessment and management (Pappalardo et al., 2020).

The E-FCR user experience is based on gamification; "the use of game design elements characteristic for games (rather than play or playfulness) in non-game contexts" (Kirkov et al., 2020, p.29). Gamification thus, provides experiences of social engagement, which in turn feeds into how we look for competition between individuals or teams (Dankbaar et al., 2017; Skerlavaj, Dimovski, & Desouza, 2010). Team projects, group learning opportunities, competition, cooperation, collaboration, and freedom of choice promote organizational learning (Ruoslahti & Trent, 2020) and co-creation (Ruoslahti, 2018).

Cyber-threat lists may be based on previous incidents, threat assessments from e.g. industry/standardization/governmental bodies, and information from social media and other available sources and repositories can provide augmenting information that helps rapidly draw conclusions to build timely cyber situational awareness (Pöyhönen et al., 2020). "The E-FCR platform should search for current technological threats and vulnerabilities on the internet by collecting information of the high priority vulnerabilities. Moreover, it should regularly check the latest available products and capabilities of all Cyber Range providers in the marketplace" (Kirkov et al., 2020, p.35).

## 5. Conclusions and suggestions

ICT is becoming more and more pervasive in the healthcare sector including computerized systems for automation of diagnostic and collection of patient data. Sensors and medical devices with IP addresses are connected to the Internet (IoT). Multidisciplinary teams interact with patient and share sensitive data also through personal devices. Predefined security requirements facilitate the creation of baselines for services and achieving desired levels of security. NCSC-FI requirements and ENISA guidelines for procurements encourage healthcare organisations set requirements for vendors. These requirements and recommendations are well structured and easy to follow but require revision and professional assessment for each procurement as nor NCSC-FI or ENISA guidelines are definite for all organisations. It is an important to verify that vendors truly meet the security requirements throughout the service or product lifecycle.

Examples of use-cases to be implemented by the ECHO project are 1) attacks against complex medical systems (blood analysis laboratory), and 2) attacks against connected physical medical devices. ECHO will create at least two sector-specific cyber-range to support healthcare-sector demonstration cases: 1) HC Cyber-Range (blood analysis laboratory) which is already ready in RHEA premises, 2) the other cyber range will leverage several medical devices. Taking into account lessons from SHAPES should enrich the ECHO demonstration cases.

## Acknowledgements

This work was supported by the ECHO project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

## References

Dankbaar, M. et al. 2017. Comparative effectiveness of a serious game and an e-module to support patient safety knowledge and awareness. BMC Medical Education. https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-016-0836-5

ENISA. 2020. Procurement Guidelines for Cybersecurity in Hospitals. European Union Agen-cy for Cybersecurity. https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

ENISA. 2015. Security and Resilience in eHealth Infrastructure and Services. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

European Commission. 2019. "Smart and healthy ageing through people engaging in support-ive systems," [Online]. https://cordis.europa.eu/project/id/857159

Kirkov, P. et al. 2020. D4.3 Inter-Sector Cybersecurity Technology Roadmap. https://echonetwork.eu/deliverables/

McLeod, A., & Dolezel, D. 2018. Understanding Healthcare Data Breaches: Crafting Security Profiles.

Pappalardo, M. et al. 2020. D2.2 ECHO Multi-Sector Assessment Framework. https://echonetwork.eu/deliverables/

PCI Security Standards Council. 2014. Information Supplement: Best Practices for Implement-ing a Security Awareness Program.

https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Pöyhönen, J., Rajamäki, J., Ruoslahti, H., & Lehto, M. 2020. Cyber Situational Awareness in Critical Infrastructure Protection. Annals of Disaster Risk Sciences, 3(1).

Ruoslahti, H. & Trent, A. 2020. Organizational Learning in the Academic Literature – Systematic Literature Review. Information & Security: An International Journal 46, no. 1 (2020): pp. 65-78.

Ruoslahti, H. 2018. Co-creation of Knowledge for Innovation Requires Multi-Stakeholder Public Relations, in Sarah Bowman, Adrian Crookes, Stefania Romenti, Øyvind Ihlen (ed.) Public Relations and the Power of Creativity (Advances in Public Relations and Communication Management, Volume (3) Emerald Publishing Limited, pp.115 – 133.

Traficom. 2019. Information security and data protection requirements for social welfare and healthcare procurements. https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/information-security-and-data-protection-requirements-social