

CYPRUS UNIVERSITY OF TECHNOLOGY
FACULTY OF ENGINEERING AND TECHNOLOGY



Bachelor's Thesis

**Towards a trainee-centric Cyber Range Training
Platform**

Antonis Ioannou

Limassol, May 2023

CYPRUS UNIVERSITY OF TECHNOLOGY
FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF ELECTRICAL ENGINEERING COMPUTER
ENGINEERING AND INFORMATICS

**Towards a trainee-centric Cyber Range Training
Platform**

Antonis Ioannou

Limassol, May 2023

Approval Form

CYPRUS UNIVERSITY OF TECHNOLOGY

Towards a trainee-centric Cyber Range Training Platform

PRESENTED BY

ANTONIS IOANNOU

Advisor _____

Dr. Michael Sirivianos

CYPRUS UNIVERSITY OF TECHNOLOGY

LIMASSOL, MAY 2023

Copyrights

Copyright© 2023 Antonis Ioannou

All rights reserved.

The approval of the thesis by the Department of Electrical Engineering, Computer Engineering and Information does not imply necessarily the approval by the Department of the views of the writer

Acknowledgements

I would like to thank everyone who generously shared their valuable insights and ideas. More precisely, I want to express my appreciation to Dr. Michael Sirivanos for his supervision and direction during the whole thesis process, assisting me in selecting a topic and following the project toward fulfillment. I would like to thank Pantelitsa Leonidou for sharing her valuable suggestions and knowledge on cybersecurity in the healthcare sector. Furthermore, I am also thankful to Nikos Salamanos for sharing his ideas and assisting me through the research process. Lastly, I appreciate my family and friends' constant encouragement and support throughout the thesis process.

Abstract

In the last decades, cyberattacks have targeted the healthcare sector because of the sensitive data it handles, for instance, Personal Health Information (PHI), Electronic Health Records (EHR), medical history, financial details, prescription data, etc. This study focuses on the cyber threats that affect the healthcare sector and the vulnerabilities within the healthcare sector that make it a prime target for cyberattacks. We design a questionnaire for medical professionals and cybersecurity teams to gather relevant data about the insights of the participant's institutions to identify and address the current challenges. Also, a Cyber Range Simulation and Training platform for healthcare stakeholders is proposed with the back-end design with its components developed. We focused on presenting the platform's prototypes that offer a user-friendly approach for developing training scenarios tailored to healthcare professionals and security experts within organizations. Moreover, we propose an approach of using open-source tools to collect data from a Security Information Event Management (SIEM) tool and present the way in which these tools can work together in (1) collecting the data related to the healthcare organization into the Cyber Range Simulation and Training Platform and (2) the creation of the training scenarios based on the Cyber Range Security Assurance model of the organization.

Table of Abbreviations

Abbreviations

<i>CRSA</i>	Cyber Range Security Assurance
<i>CRST</i>	Cyber Range Simulation and Training
<i>CSLAs</i>	Cyber security-focused Service Level Agreements
<i>CUT</i>	Cyprus University of Technology
<i>CYRA</i>	Cyber Range Assurance Platform
<i>EHR</i>	Electronic Health Record
<i>EU</i>	European Union
<i>GDPR</i>	General Data Protection Regulation
<i>GNS3</i>	Graphical Network Simulator 3
<i>HIPAA</i>	Health Insurance Portability and Accountability Act
<i>NIS</i>	Network and Information Systems
<i>PHI</i>	Personal Health Information
<i>PRC</i>	Privacy Rights Clearinghouse
<i>SIEM</i>	Security Information Event Management
<i>SLAs</i>	Service Level Agreements

List of Tables

1	Requirements for the Questionnaire	18
---	--	----

List of Figures

1	Questionnaire Demographics – participants’ position in health care organization	20
2	Cybersecurity awareness in healthcare organizations	20
3	Existence of cybersecurity training in healthcare organizations: (a) Participants from all countries;	22
4	Existence of cybersecurity training in healthcare organizations - Participants from Greek organizations,	22
5	Cybersecurity topics covered in training	23
6	Main reasons a healthcare organization’s system is down	24
7	Cyber Security Monitoring Systems in healthcare organizations	25
8	Current state of cybersecurity training in healthcare organizations	26
9	Cybersecurity training - Profile of Trainers.	26
10	Cybersecurity trainees and healthcare personnel, who must participate in the training? . .	27
11	Trainee performance evaluation methods	28
12	Trainee performance evaluation metrics when using tests.	28
13	General Cyber Range Simulation and Training Process	30
14	Step 4 Training Evaluator component	33
15	KYPO Lite architecture.	34
16	Sign In page	36
17	Training Login	37
18	Training Rules	37
19	Before ”Show Hint”	38
20	After ”Show Hint”	38
21	Flag	39
22	Chat with support	39
23	Before ”Show Hint”	41
24	After ”Show Hint”	41
25	Click on table icon	42
26	Training Results	42
27	Training Feedback	43
28	Data transfer process from the healthcare organization to the platform	45
29	Scenario process	47