



UNIVERSITY OF WEST ATTICA
SCHOOL OF ENGINEERING
DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING
PROGRAM OF DOCTORAL STUDIES

PhD THESIS

Cyber Range Systems for Education and Research

Nestoras T. Chouliaras

ATHENS-EGALEO

DECEMBER 2024



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΔΙΔΑΚΤΟΡΙΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΣΥΣΤΗΜΑΤΑ CYBER RANGES ΓΙΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΡΕΥΝΑ

Νέστορας Θ. Χουλιάρης

ΑΙΓΑΛΕΩ

ΔΕΚΕΜΒΡΙΟΣ 2024

PhD THESIS

Cyber Range Systems for Education and Research

Nestoras T. Chouliaras

SUPERVISOR: Ioanna Kantzavelou, Associate Professor, Department of Informatics and Computer Engineering, University of West Attica

THREE-MEMBER ADVISORY COMMITTEE:

Ioanna Kantzavelou, Associate Professor, University of West Attica

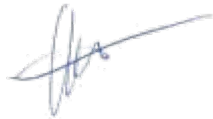
Grammati Pantziou, Professor, University of West Attica

Leandros Maglaras, Professor, Edinburgh Napier University

SEVEN-MEMBER EXAMINATION COMMITTEE

Ioanna Kantzavelou,

Associate Professor, Department of
Informatics and Computer Engineering
University of West Attica



Leandros Maglaras,

Professor,
Edinburgh Napier University

Grammati Pantziou,

Professor, Department of Informatics and
Computer Engineering
University of West Attica

Adonis Bogris,

Professor, Department of Informatics and
Computer Engineering
University of West Attica

Vassilios Mamalis,

Professor, Department of Informatics and
Computer Engineering
University of West Attica

Sokratis Katsikas,

Professor, Department of Information
Security and Communication Technology,
Norwegian University of Science and
Technology NTNU

Athanasios Kakarountas,

Associate Professor,
University of Thessaly

Examination Date 06/12/2024

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΣΥΣΤΗΜΑΤΑ CYBER RANGES ΓΙΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΡΕΥΝΑ

Νέστορας Θ. Χουλιάρης

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: **Ιωάννα Καντζάβελου**, Αναπληρώτρια Καθηγήτρια, Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, ΠΑΔΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Ιωάννα Καντζάβελου, Αναπληρώτρια Καθηγήτρια, ΠΑΔΑ

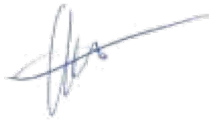
Γραμματή Πάντζιου, Καθηγήτρια, ΠΑΔΑ

Λέανδρος Μαγλαράς, Καθηγητής, Edinburgh Napier University

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Ιωάννα Καντζάβελου,
Αναπληρώτρια Καθηγήτρια,
Τμήμα Μηχανικών Πληροφορικής και
Υπολογιστών, ΠΑΔΑ

Γραμματή Πάντζιου,
Καθηγήτρια,
Τμήμα Μηχανικών Πληροφορικής και
Υπολογιστών, ΠΑΔΑ



Λέανδρος Μαγλαράς,
Καθηγητής,
Edinburgh Napier University

Αντώνιος Μπόγρης,
Καθηγητής,
Τμήμα Μηχανικών Πληροφορικής και
Υπολογιστών, ΠΑΔΑ

Βασίλειος Μάμαλης,
Καθηγητής, Τμήμα Μηχανικών
Πληροφορικής και Υπολογιστών, ΠΑΔΑ

Σωκράτης Κάτσικας,
Καθηγητής,
Norwegian University of Science and
Technology – NTNU.

Αθανάσιος Κακαρούνας,
Αναπληρωτής Καθηγητής,
Πανεπιστήμιο Θεσσαλίας.

Ημερομηνία εξέτασης 06/12/2024

Copyright © Με επιφύλαξη παντός δικαιώματος. All rights reserved.

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ και (Όνοματεπώνυμο Φοιτητή),
Μήνας, Έτος**

Η παρούσα διδακτορική διατριβή καλύπτεται από τους όρους της άδειας χρήσης Creative Commons «Αναφορά Δημιουργού Μη Εμπορική Χρήση Όχι Παράγωγα Έργα 4.0 Διεθνές» (CC BY-NC-ND 4.0). Συνεπώς, το έργο είναι ελεύθερο για διανομή (αναπαραγωγή, διανομή και παρουσίαση του έργου στο κοινό), υπό τις ακόλουθες προϋποθέσεις:

α. Αναφορά δημιουργού: Ο χρήστης θα πρέπει να κάνει αναφορά στο έργο με τον τρόπο που έχει οριστεί από το δημιουργό ή τον χορηγούντα την άδεια.

β. Μη εμπορική χρήση: Ο χρήστης δεν μπορεί να χρησιμοποιήσει το έργο αυτό για εμπορικούς σκοπούς.

γ. Όχι Παράγωγα Έργα: Ο Χρήστης δεν μπορεί να αλλοιώσει, να τροποποιήσει ή να δημιουργήσει νέο υλικό που να αξιοποιεί το συγκεκριμένο έργο (πάνω από το έργο αυτό).

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τους συγγραφείς.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον/την συγγραφέα του και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις θέσεις του επιβλέποντος, της επιτροπής εξέτασης ή τις επίσημες θέσεις του Τμήματος και του Ιδρύματος.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Ο κάτωθι υπογεγραμμένος Νέστορας Χουλιάρης του Θωμά, υποψήφιος διδάκτορας του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας και δικαιούχος των πνευματικών δικαιωμάτων επί της διατριβής και δεν προσβάλω τα πνευματικά δικαιώματα τρίτων. Για τη συγγραφή της διδακτορικής μου διατριβής δεν χρησιμοποίησα ολόκληρο ή μέρος έργου άλλου δημιουργού ή τις ιδέες και αντιλήψεις άλλου δημιουργού χωρίς να γίνεται αναφορά στην πηγή προέλευσης (βιβλίο, άρθρο από εφημερίδα ή περιοδικό, ιστοσελίδα κ.λπ.). Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Νέστορας Χουλιάρης

I dedicate this thesis to my beloved family, especially my son Thomas and my daughter Maria, whose love and encouragement have been a constant source of strength and inspiration.

Acknowledgements

Many people helped and supported me in conducting this research. First, I would like to begin by expressing my sincere gratitude to my thesis supervisor, Associate Professor Ioanna Kantzavelou, for her invaluable assistance and guidance throughout my work. I am also deeply thankful to Professor Leandros Maglaras, whose continuous support was instrumental in the completion of my PhD. I extend my heartfelt thanks to Professor Grammati Pantziou for fostering an excellent spirit of collaboration. Additionally, I am grateful to the other members of my thesis selection committee for their thorough review of my work and their valuable suggestions.

Additionally, I would like to thank the research team Information, Network and System Security (INSSEC) who helped me with research work by sharing their experience and valuable suggestions, especially Grigoris Papoutsis. I also wish to thank the Lab's technical staff, Ioannis Gialpas, Applications Lecturer Nikolaos Psarras, and Dimitrios Fergadiotis, for their assistance with technical matters and for providing access to the infrastructure of the Department of Informatics and Computer Engineering at the University of West Attica, as well as Marios Katsaros for his collaboration in the design of exercises.

Finally, I would like to express my heartfelt gratitude my job supervisor Panagiota Chouliara-Sidera and to my friends, Antonis Adamakos and Panagiotis Chalatsakos, for their invaluable support and technical expertise in Web Development and DevOps. Their assistance were essential throughout my Ph.D. journey.

Abstract

In recent years, the proliferation of cyber threats has highlighted a critical shortage of cybersecurity professionals equipped with practical, hands-on experience. The escalating frequency and sophistication of cyber-attacks underscore the urgent need for robust training solutions to bridge this skills gap. Cyber Ranges play a pivotal role in addressing this challenge by offering immersive, experiential learning environments for cybersecurity professionals.

Traditional education and certification programs often fail to equip individuals with the practical skills necessary to defend against real-world cyber attacks. Consequently, organizations remain vulnerable to sophisticated cyber threats due to the lack of skilled professionals capable of effectively mitigating these risks. Cyber Ranges provide a viable solution to this skills gap by offering hands-on training in simulated environments that mirror real-world cyber threats. By immersing participants in realistic scenarios, Cyber Ranges enable cybersecurity professionals to develop practical skills and experience in responding to various cyber-attacks. Additionally, Cyber Ranges facilitate collaboration and teamwork, fostering a dynamic learning environment conducive to skill development and knowledge sharing.

This research proposes a novel Cyber Range architecture based on container technology, aimed at addressing the limitations of current systems. It provides a comprehensive review of the existing state-of-the-art in testbeds and Cyber Ranges, identifying gaps and shortcomings that need to be addressed. The proposed architecture is designed to be flexible, efficient, and scalable, incorporating advanced features that support realistic, large-scale cyber threat simulations.

A detailed design of the proposed architecture is presented, outlining the requirements and specifications necessary for its implementation. The study explores innovative training methods using Cyber Ranges, including behavioral strategies and gamification techniques, to enhance the hands-on learning experience. Various use case scenarios demonstrate the effectiveness of the new system in realistic settings, highlighting its capabilities and the challenges encountered during implementation.

An evaluation of the system's performance is conducted through stress testing and user feedback, comparing the benefits of container-based implementations over traditional virtual machine-based systems. The results show significant improvements in scalability, adaptability, and user acceptance, underscoring the effectiveness of the proposed architecture in bridging the cybersecurity skills gap.

By offering access to realistic training environments and practical experiences, the proposed Cyber Range system empowers individuals to enhance their cybersecurity capabilities and contributes to strengthening organizational resilience against cyber attacks. The study provides insights into future research directions to further enhance Cyber Range capabilities and integration.

Περίληψη

Τα τελευταία χρόνια, η αυξανόμενη απειλή από κυβερνοεπιθέσεις έχει φέρει στο προσκήνιο την κρίσιμη έλλειψη επαγγελματιών κυβερνοασφάλειας με πρακτική και άμεσα εφαρμόσιμη εμπειρία. Η συνεχής αύξηση στη συχνότητα και την πολυπλοκότητα των κυβερνοεπιθέσεων τονίζει την επείγουσα ανάγκη για προηγμένα εκπαιδευτικά προγράμματα που θα καλύψουν αυτό το κενό δεξιοτήτων. Σε αυτό το πλαίσιο, τα **Cyber Ranges** διαδραματίζουν καίριο ρόλο, προσφέροντας διαδραστικά περιβάλλοντα μάθησης για τους επαγγελματίες της κυβερνοασφάλειας.

Τα παραδοσιακά προγράμματα εκπαίδευσης και πιστοποίησης συχνά αποτυγχάνουν να εξοπλίσουν τα άτομα με τις πρακτικές δεξιότητες που είναι απαραίτητες για να αμυνθούν ενάντια σε πραγματικές κυβερνοεπιθέσεις. Κατά συνέπεια, οι οργανισμοί παραμένουν ευάλωτοι σε εξελιγμένες κυβερνοαπειλές λόγω της έλλειψης εξειδικευμένων επαγγελματιών που μπορούν να μετριάσουν αποτελεσματικά αυτούς τους κινδύνους. Τα **Cyber Ranges** παρέχουν μια βιώσιμη λύση σε αυτό το κενό δεξιοτήτων προσφέροντας πρακτική εκπαίδευση σε περιβάλλοντα προσομοίωσης που αντικατοπτρίζουν πραγματικές κυβερνοαπειλές. Με την ενσωμάτωση των συμμετεχόντων σε ρεαλιστικά σενάρια, τα **Cyber Ranges** επιτρέπουν στους επαγγελματίες κυβερνοασφάλειας να αναπτύξουν πρακτικές δεξιότητες και εμπειρία στην αντιμετώπιση διαφόρων κυβερνοεπιθέσεων. Επιπλέον, τα **Cyber Ranges** διευκολύνουν τη συνεργασία και την ομαδική εργασία, προάγοντας ένα δυναμικό περιβάλλον μάθησης που ευνοεί την ανάπτυξη δεξιοτήτων και την ανταλλαγή γνώσεων.

Αυτή η έρευνα προτείνει μια νέα αρχιτεκτονική **Cyber Ranges** βασισμένη στην τεχνολογία των **container**, με στόχο την αντιμετώπιση των περιορισμών των τρεχόντων

συστημάτων. Παρέχει μια ολοκληρωμένη ανασκόπηση της υπάρχουσας τεχνολογίας και των **Cyber Ranges**, εντοπίζοντας τα κενά και τις ελλείψεις που πρέπει να αντιμετωπιστούν. Η προτεινόμενη αρχιτεκτονική σχεδιάστηκε για να είναι ευέλικτη, αποδοτική και κλιμακούμενη, ενσωματώνοντας προηγμένα χαρακτηριστικά που υποστηρίζουν ρεαλιστικές, μεγάλης κλίμακας προσομοιώσεις κυβερνοαπειλών.

Παρουσιάζεται λεπτομερής σχεδιασμός της προτεινόμενης αρχιτεκτονικής, περιγράφοντας τις απαιτήσεις και τις προδιαγραφές που είναι απαραίτητες για την υλοποίησή της. Η μελέτη εξετάζει καινοτόμες μεθόδους εκπαίδευσης χρησιμοποιώντας **Cyber Ranges**, συμπεριλαμβανομένων στρατηγικών συμπεριφοράς και τεχνικών **gamification**, για να ενισχύσει την πρακτική εμπειρία μάθησης. Διάφορα σενάρια χρήσης δείχνουν την αποτελεσματικότητα του νέου συστήματος σε ρεαλιστικές καταστάσεις, αναδεικνύοντας τις δυνατότητες και τις προκλήσεις που αντιμετωπίστηκαν κατά την υλοποίηση.

Η αξιολόγηση της απόδοσης του συστήματος πραγματοποιείται μέσω σεναρίων **stress testing** και ανατροφοδότησης από τους χρήστες, συγκρίνοντας τα οφέλη των υλοποιήσεων με βάση τα **containers** σε σχέση με τα παραδοσιακά συστήματα που βασίζονται σε εικονικές μηχανές. Τα αποτελέσματα δείχνουν σημαντικές βελτιώσεις στην κλιμακωσιμότητα, την προσαρμοστικότητα και την αποδοχή από τους χρήστες, υπογραμμίζοντας την αποτελεσματικότητα της προτεινόμενης αρχιτεκτονικής στην κάλυψη του κενού δεξιοτήτων στην κυβερνοασφάλεια.

Προσφέροντας πρόσβαση σε ρεαλιστικά περιβάλλοντα εκπαίδευσης, το προτεινόμενο σύστημα **ETHACA Cyber Ranges** ενδυναμώνει τα άτομα να βελτιώσουν τις ικανότητες κυβερνοασφάλειάς τους και συμβάλλει στην ενίσχυση της ανθεκτικότητας των οργανισμών απέναντι σε κυβερνοεπιθέσεις. Η μελέτη παρέχει ιδέες για μελλοντικές ερευνητικές κατευθύνσεις ώστε να βελτιωθούν περαιτέρω οι δυνατότητες και η ενσωμάτωση των **Cyber Ranges**.

Contents

Περίληψη	xī
List of Figures	xvii
List of Tables	xix
1 Introduction	1
1.1 Background and motivation	2
1.2 Challenges	4
1.3 Research objectives	5
1.4 Contributions	7
1.5 Dissertation	9
2 Literature Review	11
2.1 Related Surveys	12
2.2 Review Methodology	18
2.3 Analysis of Results	22
2.3.1 Cyber Range Objectives	25
2.3.2 Supporting Sectors of Cyber Range	27
2.3.3 Domain of Cyber Range	27
2.3.4 Type of security challenges	29
2.3.5 Educational purposes of Cyber Range	29
2.3.6 Type of environment	30

2.3.7	Infrastructure platform	31
2.3.8	Type of access	32
2.3.9	Implementation tools	32
2.3.10	Teams, Roles, and Participants	38
2.3.11	Prior Usage of the Cyber Range	39
2.3.12	Availability of Datasets	39
2.4	Challenges and Future Directions	40
2.5	Conclusions	41
3	Cyber Range Design	43
3.1	Cyber Range Architecture Model	45
3.1.1	Web fronted	46
3.1.2	Storage	47
3.1.3	Scenario	48
3.1.4	Management	49
3.1.5	Environment	51
3.1.6	Orchestration	52
3.2	Conclusions	54
4	Cyber Range Implementation	57
4.1	Infrastructure Platforms and Technologies	58
4.1.1	Infrastructure Platforms	58
4.1.2	Deployment Technologies	61
4.1.3	Deployment Frameworks	63
4.1.4	Advantages of Deploying the Kolla-Ansible Distribution	66
4.1.5	Infrastructure Environment	67
4.1.6	Learning Management System	70
4.1.7	Enhancing Monitoring and Alerting Capabilities	72
4.2	Lightweight Cyber Range Functionalities and Capabilities	74

5	Enhancing Cybersecurity Competence through Cyber Range	81
5.1	Innovative Cybersecurity Training through Cyber Ranges	82
5.1.1	Behavioral strategies	83
5.1.2	Insider Threat	85
5.1.3	Technical Controls to Identify Insider Threats	86
5.1.4	Non-Technical Approaches	89
5.1.5	Gamification	91
5.1.6	Utilization of the European Cybersecurity Skills Framework	94
5.2	Cyber Security Exercises	96
5.2.1	Design and Use of Cybersecurity Exercise Templates	97
5.3	Conclusions	98
6	Use Case Scenarios	101
6.1	WordPress injection	102
6.2	SQL injection vulnerability	103
6.3	Detect Malicious Network Traffic	104
6.4	Host Discovery and Port Scanning	105
6.5	Advanced Scanning Techniques	107
6.6	Docker Container Vulnerability Scanning	108
6.7	Vulnerability Assessment with WackoPicko	109
6.8	Conclusion	110
7	Evaluation	111
7.1	Analyzing System Performance through Stress Testing Scenarios	112
7.2	User Acceptance	116
7.2.1	Data from the survey	117
7.2.2	Results	120
7.3	Conclusion	127

8 Conclusion and Future Work	129
8.1 Conclusions	129
8.1.1 Current State-of-the-Art Regarding Testbeds and Cyber Ranges	129
8.1.2 Contemporary Architectures and Comparative Analysis	130
8.1.3 Introducing a Novel Container-Based Cyber Range Architecture	131
8.1.4 Optimizing Cyber Range Implementation	131
8.1.5 Bridging the Cybersecurity Skills Gap	132
8.1.6 Presenting Use Case Scenarios	132
8.1.7 User Acceptance and Effectiveness	133
8.2 Future Directions	133
Bibliography	137
Appendix A Publications	151
Appendix B Εκτεταμένη Περίληψη στα Ελληνικά	155
Appendix C Cyber Range Questionnaire	173
Appendix D OpenStack Kolla-Ansible Deployment	175
Appendix E Cyber Range Questionnaire	179
Appendix F Cybersecurity Exercise Template for Cyber Range System	183

List of Figures

2.1	Objectives of the Cyber Range.	27
2.2	Sectors of the Cyber Range.	28
2.3	Domains of the Cyber Range.	28
2.4	Security challenges of the Cyber Range.	29
2.5	Educational courses of the Cyber Range.	30
2.6	Types of environment.	31
2.7	Infrastructure platform.	32
2.8	Type of access.	33
2.9	Set up VMs.	33
2.10	Network topology.	34
2.11	Scoring tools for Cyber Ranges.	34
2.12	Tools to create cyber security scenarios.	35
2.13	Tools to manage.	35
2.14	Tools to monitor.	36
2.15	Network traffic.	36
2.16	User behavior.	37
2.17	Roles of participants.	38
2.18	Cyber Security Teams.	39
2.19	What type of event.	39
2.20	Dataset.	40
2.21	Dataset.	40

3.1	ETHACA Cyber Range Architecture.	45
4.1	Docker vs Virtual Machine Architecture.	62
4.2	OpenStack services	68
4.3	ETHACA Cyber Range.	69
4.4	Learning Management System	71
4.5	Prometheus	72
4.6	Grafana	73
6.1	Part of Heat Template Code at WordPress Vulnerable Scenario and Stack Topology deployed via the Horizon Dashboard.	103
6.2	Ansible sample code SQL Injection Scenario	104
7.1	Container and VM performance sample code	112
7.2	CPU Performance Comparison	114
7.3	Memory Performance Comparison	115
7.4	Execution Time Comparison	115
7.5	Decrease resource consumption VM vs Container (%)	116
7.6	Years Involved in Cybersecurity	120
7.7	Participation in Cybersecurity Exercises	121
7.8	Types of Cybersecurity Exercises Participated In	122
7.9	Previous Engagement with Cyber Range	123
7.10	Desired Cybersecurity Categories	123
7.11	Experience with ETHACA Cyber Range	125
7.12	Importance of Incorporating a Cyber Range	125
7.13	Assessment of Working Environment	126
7.14	Overall Helpfulness	127

List of Tables

2.1	Related surveys on Cyber Ranges and TestBeds	18
2.2	Summary of Cyber Ranges and TestBeds	23
2.3	Cyber Ranges features	24
2.4	Cyber Ranges tools	26
4.1	Comparison of Cyber Ranges Capabilities.	76
4.2	Features of ETHACA Cyber Range.	77
4.3	Minimum requirements of OpenStack Kolla-Ansible AIO deployment for a proof-of-concept environment.	79
7.1	Resources consumption by running ISO instances of ETHACA Cyber Range.	113
7.2	Resources consumption by running container instances of ETHACA Cyber Range.	113
7.3	Capacity of compute, memory and storage of VM.	113

Chapter 1

Introduction

In the digital era, the fabric of our global society is increasingly woven with threads of technology, making cybersecurity not just a matter of informational security but a cornerstone of national and international security [1]. The frequency and impact of cyber-attacks have escalated dramatically, targeting vital infrastructures, corporations, and even nations, with consequences that ripple across all facets of society. This escalation underscores a critical, urgent need for robust cybersecurity education and research. The development of effective strategies to combat cyber threats and ensure the resilience of our digital infrastructures is paramount [2]. Against this backdrop, Cyber Range (CR) systems emerge as quintessential tools in the arsenal for cybersecurity training and research.

Cyber Ranges are sophisticated, simulated environments designed to mirror the complex nature of real-world IT and network infrastructures, providing a sandboxed arena where cyber threats can be emulated, studied, and counteracted. These state-of-the-art platforms facilitate a hands-on approach to cybersecurity, allowing learners and researchers to hone their skills, develop new countermeasures, and thoroughly understand the anatomy of cyber-attacks in a controlled, yet realistic setting. By simulating cyber-attacks, defense mechanisms, and even the cascading effects of breaches on digital systems, CR systems play a pivotal role in preparing the next generation of cybersecurity professionals and advancing the field of cybersecurity research [3]. Traditional approaches often rely heavily on theoretical knowledge, offering limited opportunities for practical application. In contrast, CR systems

enable a dynamic, interactive learning experience that bridges the gap between theory and practice. They offer a platform for rigorous training and research, pushing the boundaries of what is possible in cybersecurity education and experimentation [4].

As cyber threats continue to evolve in complexity and scope, the importance of CR systems in developing effective cybersecurity strategies becomes increasingly apparent. These systems not only equip learners with the necessary skills and knowledge to protect digital assets but also provide researchers with a versatile tool for exploring innovative cybersecurity solutions. In this light, the exploration of cyber range systems within the realms of education and research is not just timely but essential, heralding a new era in the fight against cyber threats [5]. This dissertation delves into the development, implementation, and evaluation of CR systems, aiming to illuminate their potential and pave the way for their enhanced utilization in cybersecurity education and research.

In recent years cyber attacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated. Critical National Infrastructures are the main targets of cyber attacks, as essential information or services depend on their systems, and their protection becomes a significant issue that concerns both organizations and nations [6–9]. Attacks on such critical systems include penetrations into their network and the installation of malicious tools or programs that can reveal sensitive data or alter the behavior of specific physical equipment [10].

1.1 Background and motivation

The inception of Cyber Range systems marks a significant evolution in the domain of cybersecurity, transitioning from rudimentary network testing environments to sophisticated platforms that simulate complex cyber ecosystems. This journey reflects the shifting landscape of cybersecurity threats and the growing necessity for advanced defense mechanisms. Initially, the concept of cyber range was similar to traditional network testing environments, focusing primarily on assessing the robustness of network defenses against a limited set of vulnerabilities. These early iterations were essential to understand network vulnerabilities

and the basics of intrusion detection, but did not capture the multifaceted nature of modern cyber threats. As the internet and digital technologies proliferated, the complexity and sophistication of cyber-attacks escalated, prompting a paradigm shift towards more dynamic and comprehensive training and research solutions.

Today's cyber ranges are designed to mimic real-world IT infrastructures, applications, and services, incorporating the latest in virtualization technology and simulation techniques. These environments provide a realistic backdrop against which a wide array of cyber threats can be emulated and counteracted, ranging from simple malware injections to sophisticated, state-sponsored cyber-attacks.

In the realm of education, CR systems have revolutionized the way cybersecurity is taught. Beyond theoretical knowledge, they offer students and trainees hands-on experience in detecting, responding to, and mitigating cyber threats. This experiential learning approach is invaluable in developing the practical skills necessary to navigate the complexities of today's cybersecurity landscape. Students are not only taught how to use tools and techniques but are also challenged to think critically and adaptively, mirroring the real-world scenarios they will encounter in their professional lives.

Similarly, in research, CR systems serve as indispensable tools for investigating the nuances of cyber threats and the effectiveness of countermeasures. Researchers utilize these platforms to conduct controlled experiments, test new defense mechanisms, and study the behavior of malware in a safe environment. This ability to simulate realistic cyber-attacks and defenses offers insights that are critical to advancing the field of cybersecurity. Moreover, CR systems facilitate interdisciplinary research, bridging the gap between technical cybersecurity solutions and their implications for policy, ethics, and law.

The evolution of CR systems from simple testing environments to complex simulators of cyber ecosystems signifies a critical advancement in our approach to cybersecurity education and research. By providing a realistic, hands-on experience, these systems play a pivotal role in preparing the next generation of cybersecurity professionals and advancing our understanding of cyber threats and defenses. As we continue to confront increasingly sophisticated

cyber-attacks, the importance of CR systems in developing resilient cybersecurity strategies cannot be overstated.

1.2 Challenges

Despite significant advancements in Cyber Range (CR) systems, several challenges and gaps persist, hindering their full potential in cybersecurity education and research. These issues revolve primarily around scalability, adaptability, and integration with existing technological and educational frameworks, posing substantial obstacles to the effective use and widespread adoption of CR systems.

- **Scalability Challenges:** As cyber threats grow in complexity and volume, the demand for CR systems to simulate these threats in real-time and on scale has become paramount. Current CR systems often struggle with scaling to accommodate large numbers of users simultaneously or to replicate large-scale cyber ecosystems accurately. This limitation restricts the ability of educational institutions and research organizations to provide comprehensive training and conduct extensive research, particularly when exploring large-scale cyber incidents or testing the resilience of networks under high-stress scenarios.
- **Adaptability Issues:** The dynamic nature of the cybersecurity landscape necessitates CR systems that can quickly adapt to emerging threats and evolving technology standards. However, many existing systems lack the flexibility needed to update or modify simulations and environments promptly. This inflexibility can lead to outdated training scenarios that do not reflect the latest threat vectors or technological advancements, diminishing the effectiveness of cybersecurity education and preparedness.
- **Integration with Technological and Educational Frameworks:** Effective integration of CR systems within existing technological infrastructures and educational curricula remains a significant challenge. Many CR systems operate in isolation, without seamless integration into learning management systems (LMS), educational tools,

or the broader IT infrastructure of an organization. This disjointedness complicates the user experience, limits access to cyber range functionalities, and hampers the ability of educators to incorporate hands-on cybersecurity training into their teaching methodologies.

Given these challenges, there is a pressing need for research and development into more flexible, scalable, and accessible CR architectures. Such architectures should be designed with the capacity to simulate a wide array of cyber threats at scale, allowing for the accommodation of a large number of simultaneous users without compromising the fidelity or complexity of the simulation.

Furthermore, they must be adaptable, enabling quick updates and modifications to reflect the latest cyber threats and technological developments. Lastly, integration capabilities must be prioritized, ensuring that CR systems can be seamlessly embedded within existing technological and educational frameworks, thereby enhancing accessibility and usability for both educators and learners.

Addressing these gaps requires a concerted effort to innovate and rethink the design and implementation of CR systems. By developing CR architectures that are more aligned with the needs of contemporary cybersecurity education and research, we can significantly enhance the preparedness of future cybersecurity professionals and the efficacy of cyber defense strategies.

1.3 Research objectives

This dissertation aims to address the pressing challenges faced by current Cyber Range (CR) systems, as identified in the problem statement, through the development of a novel CR system architecture. The primary goal is to enhance the scalability, adaptability, and integration capabilities of CR systems, thereby significantly improving their effectiveness in cybersecurity education and research. To achieve this overarching aim, the research is structured around several specific objectives:

Conduct a Comprehensive Comparative Analysis of Existing CR Systems: To lay the foundation for this research, an extensive review and comparative analysis of current CR systems will be undertaken. This analysis will focus on evaluating the systems' scalability, adaptability, and integration capabilities with existing technological and educational frameworks. The objective is to identify the strengths and weaknesses of current systems, providing critical insights that will inform the design of the novel CR architecture.

Design a Novel CR System Architecture: Based on the insights gained from the comparative analysis, the next objective is to design a novel CR system architecture. This architecture will specifically address the identified limitations by incorporating advanced scalability features, ensuring flexibility for updates and modifications, and facilitating seamless integration with educational and technological infrastructures. The design process will involve the formulation of detailed specifications that align with the requirements for effective cybersecurity training and research.

Develop and Implement the Proposed CR System Architecture: Following the design phase, the proposed CR system architecture will be developed and implemented. This objective encompasses the technical realization of the CR system, ensuring that the theoretical design translates into a functional, scalable, and adaptable platform. The development process will pay close attention to the integration capabilities, aiming to create a CR system that can be easily embedded within existing educational and technological environments.

Evaluate the Effectiveness of the Novel CR System in Education and Research Settings: The final objective involves a comprehensive evaluation of the newly developed CR system's effectiveness within both educational and research contexts. This evaluation will assess the system's scalability, adaptability, and integration capabilities in real-world scenarios, measuring its impact on enhancing cybersecurity training and research outcomes. Criteria for evaluation will include user feedback, performance metrics, and the system's ability to simulate a wide range of cyber threats accurately and at scale.

Provide Recommendations for Future CR System Development: Based on the findings from the evaluation phase, the dissertation will conclude with recommendations for future development and research in the field of CR systems. These recommendations will aim to

guide ongoing efforts to refine and enhance CR systems, ensuring they remain effective tools for combating the ever-evolving landscape of cyber threats.

Achieving these objectives will contribute significantly to the field of cybersecurity education and research, offering a more effective, scalable, and adaptable CR system architecture that better meets the needs of learners, educators, and researchers in the digital age.

1.4 Contributions

The proposed dissertation aims to undertake a comprehensive investigation into existing Cyber Range systems tailored for academic, governmental, military, and private sectors. This study will encompass an in-depth analysis of the environments offered, the intricacies of simulated networks, the scope of training provisions, and the array of functionalities provided by these systems. These functionalities include personalized scenario creation, vulnerability exploitation methods, development platforms, tools, and techniques utilized for mitigating cyber threats. Through meticulous scrutiny and evaluation, this research endeavors to enrich our understanding of Cyber Range systems and their pivotal role in bolstering cybersecurity readiness across diverse sectors.

The significance of this research in developing a novel Cyber Range (CR) system architecture cannot be overstated, especially in the context of the escalating complexity and frequency of cyber threats facing our global digital infrastructure. This research directly addresses the critical need for enhanced cybersecurity training, aiming to equip current and future cybersecurity professionals with the skills and knowledge necessary to defend against and mitigate cyber threats effectively.

The proposed CR system architecture promises to revolutionize cybersecurity training by providing a more scalable, adaptable, and integrated platform for hands-on learning. By overcoming the limitations of current CR systems, this research seeks to offer a more immersive and realistic environment for cybersecurity training. This environment will not only facilitate the simulation of a wide array of cyber threats but also enable learners to engage in real-time threat detection, response, and mitigation exercises. The practical experience

gained through this advanced training is invaluable, ensuring that learners are not merely familiar with theoretical concepts but are also adept at applying their knowledge in real-world scenarios. Consequently, this research holds the potential to significantly elevate the quality of cybersecurity education, preparing a workforce that is more capable of addressing and adapting to the evolving cybersecurity landscape.

In addition to its implications for education, the development of a novel CR system architecture represents a significant advancement in cybersecurity research. By providing a more flexible and comprehensive platform for the simulation and study of cyber threats, this research enables a deeper understanding of cybersecurity vulnerabilities and defense mechanisms. Researchers will benefit from the ability to conduct more nuanced and extensive investigations into cyber threats, leveraging the CR system to test and refine new cybersecurity technologies and strategies. This enhanced research capacity is critical for staying ahead of cybercriminals, fostering innovation in cybersecurity defense measures, and ultimately contributing to the development of a more secure digital world.

This dissertation makes a significant contribution to the field of cybersecurity by developing and evaluating a new architecture for cyber ranges. Utilizing modern technologies and approaches, this research aims to improve cybersecurity education and research by offering a flexible, efficient, and scalable system. The contributions of this dissertation range from reviewing existing technology and proposing a new architecture to the practical implementation, use case scenarios, and evaluation of the system's performance and user acceptance.

The contributions encompass:

- Presents the current state-of-the-art testbeds and cyber ranges.
- Presents the findings of a set of structured interviews with organizations that have a testbed and cyber range.
- Provides a comparison of the features and tools used in modern cyber ranges.
- Discusses the findings and gives insights of modern cyber ranges.

- Provides a comparable presentation of Cyber Range platform environments, and key design and implementation features are identified and explored,
- A novel lightweight, flexible, and adaptable Container-based Cyber Range architecture is proposed,
- The design of the proposed Cyber Range platform architecture is illustrated and detailed descriptions are provided for the six modules that comprise it,
- Presents the implementation and technical details demonstrating the advantages and benefits of open-source cloud platform application using primarily containers,
- Explores Use case scenarios to address operational challenges, demonstrating the platform's strengths in performance, scalability, costs, and resource allocation.
- Presents ETHACA Cyber Range and highlight its key features.
- Demonstrates cyber security exercises specifically designed and developed for the ETHACA Cyber Range.
- Presents the findings from a comprehensive questionnaire developed in collaboration with cybersecurity experts, researchers, and students.

1.5 Dissertation

The dissertation roadmap provides a structured overview of the forthcoming chapters, guiding readers through the systematic exploration of Cyber Range (CR) systems. Each chapter is meticulously crafted to address specific facets of CR development, from theoretical foundations to practical implementation and evaluation. By following this roadmap, readers will gain a comprehensive understanding of CR architectures, integration challenges, use cases, and future research directions.

Chapter 1 presents the background, motivation, and objectives of the research. It introduces the critical need for advanced cybersecurity training and proposes Cyber Range systems as a viable solution.

Chapter 2 provides a comprehensive review of existing Cyber Range systems and testbeds. It identifies the strengths and weaknesses of current solutions and highlights gaps that the proposed research aims to fill.

Chapter 3 proposes a novel Cyber Range architecture based on container technology. It provides detailed descriptions of the requirements, specifications, and the six key modules that constitute the proposed system.

Chapter 4 presents the practical aspects of implementing the proposed ETHACA CR architecture. It provides a comparison with existing systems, emphasizing the benefits and detailing the tools and technologies used in development.

Chapter 5 explores innovative training methods using Cyber Ranges. It presents behavioral strategies and gamification techniques, highlighting the importance of hands-on experience in cybersecurity education.

Chapter 6 provides various use case scenarios to demonstrate the effectiveness of the new Cyber Range system. It illustrates how the system can be applied in realistic settings to enhance cybersecurity training and research.

Chapter 7 presents an evaluation of the system's performance through stress testing and user feedback. It provides a comparative analysis of container-based versus virtual machine-based implementations, highlighting efficiency and scalability improvements.

The final chapter 8 provides a summary of the research findings, discussing the current state-of-the-art and the proposed system's contributions. It outlines future research directions to further enhance Cyber Range capabilities and integration.

Chapter 2

Literature Review

The exponential increase in cyber threats [11] has underscored the need for advanced training and research methodologies to effectively prepare cybersecurity professionals. Traditional educational frameworks have struggled to keep up with the rapidly evolving cyber threat landscape, often lacking practical, hands-on experience. To address this gap, there is a critical requirement for training activities and environments capable of supporting challenging scenarios, complemented by clear guidance, procedures, and tools. Such environments can empower individuals to respond collectively and collaboratively to diverse and unpredictable situations. This environment should blend simulations and emulations of real components and systems, embed different attack and defense mechanisms [8], [12] and must be able to adapt to a variety of different incidents, to be cost-effective and attractive for organizations and educational institutes.

CRs have emerged as a solution to this challenge, offering advanced features and capabilities beyond simple simulation environments. CRs are sophisticated exercising environments that contain both physical and virtual components, enabling the representation of realistic scenarios for training purposes [13]. These environments are designed to closely mimic real-world conditions, providing a robust platform for developing and testing cybersecurity skills. Carnegie Mellon University [14], through its Software Engineering Institute (SEI), has developed open-source software tools that create secure and realistic cyber simulations. These tools are integral to modern CRs, as they allow for the recreation of real-world condi-

tions, making training exercises more realistic and effective. By incorporating such advanced technologies, CRs can offer a comprehensive and immersive training experience that equips cybersecurity professionals with the necessary skills to handle complex cyber threats.

We present the current state-of-the-art on testbeds and CRs that are used for training and research purposes. A systematic review of the literature on CR systems was carried out and the study revealed that there is a variety of implementations with different approaches that have been developed in different environments, using real, virtual, or hybrid equipment. Moreover, to better understand what are the important components of a modern CR, we conducted structured interviews with technical directors who have developed and used recent CRs and presented the findings.

The findings of the research will be a guide for the effort to design, develop, and implement a CR platform for the University of West Attica (UNIWA) but can also be a guide for other CRs that are under development. The aim of a modern CR should be to enhance courses with hands-on experience for participants. Also, will enhance the research goals of the university by using a more complex and realistic environment than currently has. UNIWA has a cybersecurity team (INSSec) with active participation in national and international cybersecurity exercises over the last decade as well as Capture the Flag (CTF) competitions such as UniCTF 2019 and UniCTF 2020. Also, organized the CTF competition [15] UniwaCTF 2019, a competition between Greek universities. A CR system will enhance the realism of CTF contests, allowing UNIWA to organize more complex cyber exercises, such as blue vs. red team.

2.1 Related Surveys

During the literature review conducted between March and June 2020, numerous cyber ranges and testbeds were identified across various domains, including education, CTF challenges, industrial control systems, cyber-physical systems, and Supervisory Control And Data Acquisition (SCADA) environments.

Davis and Magrath (2013) [16] conducted a survey of CRs and classified their findings into three categories: Modeling and Simulation, Ad-hoc or Overlay, and Emulations. Specifically, their survey had the purpose of assisting organizations to select and build their desired CR capability. Hence, they surveyed the available options for constructing and managing a CR, for monitoring and analysis, training scenarios, communities for collaboration, and commercial offerings. They categorized CR using a two-level model. Firstly, they distinguished the CRs by their type, such as Simulation, Ad-hoc or Overlay, and Emulation. They also named the fourth category as Analytics without actually using it. Following previously defined methodologies, they categorized a CR as simulation when utilizing software models of real cases, as overlay if they use the real production equipment, and as emulation in the case of running the real applications on separate equipment. The second-level criteria of their categorization have been the sector the CR supports and the categories have been academic, military, or commercial. The survey makes interesting points about the above-mentioned categories. Simulation CRs are sterilized, emulation ones have more realistic behavior, but they are expensive, while overlays are only a small minority. According to the survey, the emulation CRs are the best category, especially when using virtualization. Moreover, the survey states that the main use of CRs is training, leaving far behind cybersecurity testing and research and development. This survey is quite broad as it covers almost 30 CRs, and it fulfills its aim. It refers widely to military-developed and operated cases. This is expected as, at the time, military implementations had quite a few operating CRs. However, this survey is already seven years old, meaning that a lot of things have changed since. Moreover, it overlooks the cases where several categories are combined in hybrid cross-category environments.

Holm (2015) [17] surveyed 30 ICS testbeds. This survey has been a part of a study about critical infrastructures and eventually refers specifically to Industrial Control Systems (ICS). The study was motivated by the increasing vulnerability of ICS to cyber-attacks. It was titled “Virtual Industrial Control System Testbed” and was performed for FOI, the Swedish Defense Research Agency. The main purpose of the study was to specify the way to create a high-fidelity Virtual Industrial Control System (VICS) and the first step was surveying the

existing relevant testbeds through five Research Questions. The expected outcome would be the creation of a new testbed (CRATE). The survey collected information from 30 ICS testbeds in 12 countries. The study covers several testbed characteristics like the three methods that can be used to implement ICS in testbeds (virtualization, simulation, and hardware), including relevant subcategories (Operating System virtualization, Programming Language virtualization, Library virtualization) and categorization of these testbeds' objectives into 11 categories (Vulnerability analysis, Education, Tests of defense mechanisms, Power system control tests, Performance analysis, Creation of standards, Honeynet, Impact analysis, Test robustness, Tests in general, Threat analysis). Furthermore, the survey presents per category how the reviewed 30 testbeds implement their control center, communication architecture, field devices, and observed/controlled processes. The available categories are again Virtualization, Simulation, Emulation, and Hardware. However, this survey leaves room for hybrid methods. In addition, the survey states Fidelity, Repeatability, Measurement Accuracy, and Safe execution of tests as the basic requirements that testbeds should comply. It is clarified though that these requirements are not a product of the survey itself, but they pre-existed. The survey concludes that none of the questioned testbeds implements an overlay model (enables executing a real field device inside a virtual/emulated container). The complexity of ICS accounts for this conclusion. Finally, it distinguishes vulnerabilities as Policy and Procedure Vulnerabilities, Platform Vulnerabilities, and Network Vulnerabilities. Finally, the survey describes the architecture and functionality of a designed testbed (CRATE). This survey follows a stable methodology, approaching the testbeds from various angles. Moreover, the analysis has taken into account a satisfactory amount of 30 testbeds. However, its main focus is the industrial (ICS) testbeds, and, eventually, the results are narrowed to this specific category of testbeds. In addition, since the time of the survey (2015), ICS systems have become more connected and have revealed more surface to the attackers. Unavoidably, the survey and its vulnerability analysis haven't taken into account the evolved and interconnected situation nowadays.

Yamin [18] presents a survey of CRs and security testbeds and provides a taxonomy and an architectural model of a generic CR. Their work begins with the definition of a cyber

exercise where they define the stages of such an exercise as well as the teams involved (white, blue, red). They identify a gap in existing surveys as they characterize them as sectorial or outdated. The chosen methodology of this survey has been the systematic literature review which consists of eight stages (Statement of purpose, protocol establishment, a search of the sources, screening of the literature, assessment, data extraction, synthesis of the outcome, and review). During this process, they produce an initial taxonomy where a CR consists of five basic pillars (scenario, monitoring, teaming, scoring, and management). Indicative of the width of the survey is the variety of cyber exercise teams/roles they have identified (red, blue, white, orange, purple, yellow, green, autonomous). An outcome of the survey is a classification of the capabilities and functionalities of modern CRs, as well as a new taxonomy based on the information gathered, with six pillars (scenario, monitoring, learning, management, teaming, environment), has been produced. The survey has researched and recorded a multitude of simulation, emulation, hardware, management, monitoring, traffic generation, and other relevant tools and solutions implemented in contemporary CRs. In addition, the functional architecture of a generic CR is described on the surveyed CRs, the survey attempts to predict the future shape of the CR environment. This survey is, by all means, an impressive work that firstly analyses and then combines data from multiple papers mainly for the period 2015–2017. The survey performs a wide approach and analysis of the literature. However, the survey concludes in a rather conservative manner, and the predicted future CRs don't quite differ from the present ones.

Kucek (2020) [19] investigates the underlying infrastructures and CTF environments, specifically open-source CTF environments, and examines eight open-source CTF environments. The survey aims to be used as a valuable reference for whoever is involved in CTF challenges. Starting from 28 platforms, the survey shortlisted 12 open-source environments and finally managed to examine eight of them (CTFd, FacebookCTF, HackTheArch, Mellivora, Pedagogic-CTF, PicoCTF, RootTheBox, WrathCTF), and to extract valuable conclusions and comparison data. The study was motivated by the popularity of CTF events combined with the lack of studies that examine the underlying infrastructure and configuration of real-time cyber exercises like CTFs. Once more, it starts with a questionnaire of four

Research Questions (RQs). The survey distinguished the open-source CTF environments and attempted empirical research of them. They followed an organized methodology of five comprehensive steps (general review, shortlist of open-source CTFs, installation, configuration challenges, and conclusions). To empirically examine each of the eight shortlisted environments, the survey conducted 16 different challenges categorized into five CTF types (quiz, jeopardy, Attack-defense, Mixtures, King of the Hill). Some interesting results include the architecture of the platforms. Some of them run on a certain O/S, while others run on any O/S. The next (higher) layer above the O/S is either the container layer or the virtualization one. The CTF challenges are configured on top of these layers. The survey concludes that the examined environments differ in some features they support and the respective configurations that are available. All the examined platforms have some generic features (participant registration, challenge provision, user manual, scoring methodology). The platforms differ in the specifics and the available options of the mentioned features. The survey has been both original and ambitious to deepen the performed analysis. However, its main objective is the CTF implementations and, consequently, it is narrowed to this specific category of testbeds. Moreover, the actual research is limited to eight CTF environments. Starting from around 30 candidate CRs, they finally realized the empirical study on eight of them because of various reasons (proprietary environments, lack of adequate documentation, etc.).

Ukwandu [20] presents a survey of CRs and security testbeds. In this very recent survey, only publications from selected databases and only from the last five years (2015–2020) are examined. A taxonomy is developed to provide a broader comprehension of the future of CRs and testbeds. The paper makes multiple references to the smart-everything technological transformation which must be taken into account when assessing or training in cybersecurity. Once more, the following approach has been the chain: plan, select, extract, execute. The survey is presented as an overview of the CRs and Test Beds which can be found in the literature and 44 CRs are identified. These instances are categorized in multiple ways, initially based on their application (Military/Defense/intelligence, Academic, Commercial, Law Enforcement, etc.) and their type (Private, Public, Federated).

In addition, the teaming options are presented. The survey presents a classification of the found CRs according to their implementation method (Emulation, Simulation, Overlay, Live). The survey describes in fair detail the architecture and interconnection of CR building blocks. The survey defines a CR scenario and then different scenario options and differentiation factors (design, validation, deployment) are described. The stages that a training testbed should include are presented in an impressively simple but straightforward plan. The different approaches to training are described (gamification, Mock Attack Training, Role-Based Training, and exercises). The survey argues in favor of the differentiation between CRs and Test Beds. It presents CRs as far more complicated than Testbeds. This argument concludes with the need for different taxonomies, respectively. Finally, according to the survey, the future shape of CRs and Test Beds is going to combine real-time, intelligent implementations featuring mobility, automatic configuration, and integration of different technologies, applications, and appliances. Throughout this extensive analysis, the survey doesn't avoid some minor contradictions. Moreover, our survey integrates a structured interview that has been performed on a selected group of representative CRs.

As shown in Table 2.1, we classify the surveys according to the following criteria:

- Focus area: We categorize surveys in relation to their scope.
- Method: this category indicates the method of collection and analysis of the data that are related to the CRs.

Most of the surveys, including ours, have a broad scope, while only two of them were focused on a specific area of research, ICS and CTFs. The main difference between our survey as compared to the previous ones is the use of mixed data collection methods that included both a literature review and structured interviews with Universities and agencies that have deployed and run such CRs. This method helped us cover the lack of published information in terms of architecture, topology, and tools.

Table 2.1 Related surveys on Cyber Ranges and TestBeds

Survey	Reference	Systems studied	Focus Area	Year	Method
Davis-Magrath et al.	[16]	30	Broad	2013	Literature Review
Holm et al.	[17]	30	ICS	2015	Literature Review
Yamin et al.	[18]	100	Broad	2019	Literature Review
Kucek et al.	[19]	28	CTFs	2020	Empirical Review
Ukwandu et al.	[20]	44	Broad	2020	Literature Review
Chouliaras et al.	[21]	25	Broad	2021	Literature Review, Structured Interviews

2.2 Review Methodology

This study systematically identifies and critically analyzes State-Of-The-Art CRs. The methodology employed involves an exhaustive analysis of pertinent literature and the synthesis of research findings in a systematic, transparent, and reproducible manner. What sets our survey apart from previous ones is the utilization of mixed data collection methods, incorporating both a comprehensive literature review and structured interviews with universities and agencies that have implemented and operated such CRs. This approach was instrumental in addressing the lack of published information regarding architecture, topology, and utilized tools.

Among many cyber incidents that have occurred in the last decade, two of them can be considered as major triggers for the development of CRs firstly the attack against the nuclear program of Iran [22]. This attack which was revealed in 2010 used the computer worm Stuxnet and specifically targeted the Programmable Logic Controllers (PLCs) used to automate machine processing systems. Since then, the malware has been mutated and discovered in other industrial and energy installations. Secondly, on 23 December 2015 via a series of cyber-attacks, cyber attackers remotely controlled the Ukrainian power grid [23], specifically the SCADA distribution management system, and eventually caused a significant power outage to the Ukrainian constituency. The above-mentioned incidents have been more

than persuasive of the vulnerability of industrial systems. This resulted in widely opening the way for the development of CRs.

Initially, an up-to-date survey of the present situation of CR systems was conducted. This survey has revealed multiple useful outcomes. Some of them are the characteristics of modern CRs and testing beds, the various development platforms used, the tools and methods that are implemented, how fast the implementations occur, how are the exercises conducted and executed, how are the relevant scenarios created and implemented, etc.

Apart from the need to test and evaluate the cybersecurity aspect of applications, tools, and systems, CRs are extremely useful for the capacity building of cyber experts. They must develop and possess several abilities like being deeply technically skilled, capable of recognizing and responding to complicated and urgent situations, able to assess risks and vulnerabilities, handling uncertainty, to solving problems to provide explanations to thinking adversarial. In a nutshell, today's security experts must possess a "security mindset" as described in [24].

Various definitions of CRs have been given in the relevant literature and publications. The definition given in NIST one-pager [25] has been chosen as the first among equals. Thus, according to NIST, CRs are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet-level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.

The research performed reveals that the environment of CRs in terms of their development can be categorized into three main types: simulation, emulation, and hybrid. A Simulation involves using a model, a virtual instance to recreate a complex network environment based on the real network components' behavior. Emulation is when the CR runs on the dedicated physical network infrastructure of the CR. Hybrid emerges from a customized combination of any of the above types. An additional category refers to overlay CRs which are the instances that run in parallel with the actual production systems on the real equipment and infrastructure.

We can also categorize CRs based on their operator. The main players in the development of CRs and similar testbeds have been universities, government agencies, military research centers, international organizations, and their affiliates. While the details of some CRs are publicly available, there also exist CRs that are funded by the military and governments throughout the world and their details are eventually classified. Throughout the recent development and widening of the CR constituency, the concept of a federation of CRs has emerged. The concept of federation relies on the consideration that a single CR would have enormous costs and would be extremely complicated if it were to have all the necessary features and functionalities, the whole package. Therefore, it would be better organized, and also modular, and in effect realistic, if multiple CRs, each within a specific area of expertise, could collaborate to offer to their users a wide variety of use cases and different scenarios. For example, some CRs simulate social media networks or publicly available internet resources while other CRs may be specialized in simulating industrial control systems or critical infrastructures. The combination of the capabilities of different CRs would result in the development of a much broader simulation environment available for their end-users, while at the same time, the overall cost would remain unchanged. Following this concept, several CR federations are being developed. Such an example is the CRs Federation project which aims at building an EU-wide CR. Participants of this federation include eleven EU member states, the European Space Agency (ESA) as well as the European Defence Agency (EDA). Another relevant initiative is the CyberSec4Europe project which refers to designing, testing, and demonstrating potential governance structures for a future European Cybersecurity Competence Network. One more example is the ECHO project (European network of Cybersecurity centers and competence Hub for innovation and Operations) launched by the European Commission with the vision to establish and operate a Cybersecurity Competence Network.

The Deployment models of cloud computing are categorized into four commonly used categories. Private Cloud, Public Cloud, Community Cloud, and Hybrid Cloud. Additionally, there are three Service models of Cloud Computing: Infrastructure, Software, and Platform as a Service (IaaS, SaaS, PaaS). In the SaaS model, a software provider sells a software

application that can be used on-demand. In the IaaS, the provider offers as service computing resources like storage, servers, or peripherals. The users can have a virtual server in a very short time, and they pay only for the resources they use. The PaaS model represents an abstraction layer between the IaaS and SaaS and its target group includes deployers and developers. Infrastructure platforms and tools include OpenStack [26], Opennebula [27], Proxmox [28], VMware [29], Public cloud (AWS), Minimega [30] and KVM [31].

Infrastructure as code (IaC) is another step ahead towards infrastructure agility and flexibility. With IaC, the management of infrastructure (networks, virtual machines, load balancers, and connection topology) is realized in a descriptive model. Some Infrastructure as code (IaC) tools that we came across in our survey include Chef [32], Puppet [33], Ansible [34], SaltStack [33], Terraform [35], and Vagrant [32].

In the present paragraph, some terms that are necessary for the forthcoming analysis are defined. When we talk about deployment, we refer to the process of putting a new application, or a new version of an application, to run on a prepared application server. Orchestration is the arrangement or coordination of multiple systems that are designed to cooperate. Provisioning (used by DevOps) refers to getting computers or virtual hosts to use and installing needed libraries or services to them. Configuration management (CM) is a system engineering process for the establishment and maintenance of a product's performance, functional, and physical attributes with its requirements, design, and operational information. Configuration management aims to bring consistency to the infrastructure. The above-mentioned tools (Chef, Puppet, Ansible, SaltStack) are all configuration management tools, which means they are designed to install and manage software on existing servers, whereas Terraform is an orchestration tool, meaning that it is designed to provision the servers themselves, leaving the configuration of these servers to other tools. These two categories are not mutually exclusive, as most configuration management tools can do some degree of provisioning and most orchestration tools can do some degree of configuration management.

Using the CR background and environment as described in the previous paragraphs, we now move forward to explain the features of the CRs we found in our survey. We analyze 25 CRs, and discuss the features they incorporate, such as objective, environment, supporting

sector, etc (see Table 2.2). Research (R), Training (T), Exercise (E), Education (ED), Operations (O), Testing (TE), Academic (A), Military (M), Government (G), Private Enterprise (PE), Industry (I), Demonstrations (DM), Development (DV), Testing (TS), Emulation (EM), Simulation (S), Hybrid/Cyber-Physical (HCP), VMWARE (VW), OpenStack (O), Minimega (MN), TerraForm (TR), Public cloud AWS (AW), QEMU / KVM (Q), Virtualbox (VB), Custom (C), Yes (Y), No (N), Not Available (N/A), Docker (D), Instructors (IN), Provided on-demand (OD), In house (IH), On-Premise (OP), Online (ON) and On-Site (OS). Then, based on these findings, we selected the ten most representative cyber-ranges, and we moved forward with the structured interview

2.3 Analysis of Results

Due to the lack of several features that are not mentioned in the publications but also to have a better picture of the systems used, a structured questionnaire [67] was created and sent to selected universities and research centers that develop and maintain such systems (see Tables 2.2 and 2.3).

Table 2.3 includes the following information Web (W), Cryptography (C), Forensics (F), Exploitation (E), Steganography (S), DDoS (DD), APT (AP), Ransomware (R), SQL Injections (SI), Malware Analysis (MA), Reverse Engineering (RE), Risk Management (RM), Information Security Economics (ISE), Cyber Crisis Management (CM), Cyber Policy Analysis (CP), Digital Forensics (DF), Software Security (SS, ICS Security (IC), Custom (CU), Request Base (RB), Digital Forensics (DF), Network security (NS), Web Security (WS), Software Security (SS), ICS Security (IC), OT Security (OS), Hardware Security (HS), Cloud Security (CS), Data-driven cybersecurity management (CM), On Premise (OP), Remote Access (RA), Local (L), SOC (SC), NOC (NC), CERT (CR), CSIRT (CS), CISO (CO), IT-Team (IT), Legal (LG), Managers (M), C-levels (CV), BLUE (B), RED (RD), GREEN (G), YELLOW (YL), WHITE (WT), PURPLE (P),Event (EV), Workshop (WS), Exercise (EX), and Educational Institutions (EI).

Table 2.2 Summary of Cyber Ranges and TestBeds

Operator	Objective	Sector	Environment	Infrastructure Platform(s)	Dataset
NATO Cyber Range [36]	T, E	M	EM	VW	N/A
Masaryk University (KYPO) [37, 38]	R, T, E, ED	A	EM	O	Y
Florida Cyber Range [39]	ED, R, T, O	M	N/A	N/A	N/A
Sandia National Laboratories (Cyber Scorpion) [30]	T	G	N/A	MN	N/A
Virginia Tech [40, 41]	R, T, E	A	S	AW	N/A
De Montfort University [13]	R, T, E	A	HCP	Q	OD
Royal Military Academy [42, 43]	R, T	A, M	S	VB, C	N
AIT Austrian Institute of Technology [44–46]	R, T, E	A, G, M PE	HCP	O, TR	N
Naval Postgraduate School [47, 48]	T, E, ED	A, G, M	S	D	IN
Norwegian University of Science and Technology (NCR) [49, 50]	R, T, E, Ts	A, G, M, PE	EM, S, HCP	O, VB, VM, D	OD
Università degli Studi di Milano [26]	T	R	EM, S	O	No
JAMK University of Applied Sciences (JYV-SECTEC) [51, 52]	R, T, E	A, G, M, PE	EM, S, HCP	N/A	IH
Swedish Defence Research Agency (CRATE) [53, 54]	R, T, E	G, M	HCP	VB	ON
Michigan Cyber Range [55]	T	A	N/A	N/A	Yes
Silensec [56]	T	I	N/A	N/A	ON
CYBERIUM (fujitsu) [57]	T	I	N/A	N/A	ON
DECIDE (NUARI)[58]	R, T, E	A	N/A	N/A	ON
Georgia Cyber Range [59]	ED, T, R, DM, DV	A	N/A	N/A	ON
IBM X-Force Command C-TOC [60]	T, E	I	N/A	N/A	ON
Cybexer [61]	T, E	I	N/A	N/A	ON
Airbus Cyber Range [62]	R, T, E	I	S	N/A	ON
Raytheon Cyber Range [63]	T, E	M, A, I	N/A	N/A	ON
hns-platform [64]	T, E	I	HCP, S	N/A	ON
Cyberbit Cyber Range [65]	T, E	I	S	N/A	ON, OP
Cyber Warfare Range [66]	T, E	I	S	N/A	OS, OP

Table 2.3 Cyber Ranges features

Operator	Security Challenges	Courses	Access	Roles	Teams	Events
De Montfort University	W, E, AP	DF, SS, IC	OP	SC, NC, CR	B, RD, G, YL, WT, P	EV, WS, EX
Royal Military Academy	W, F, DD, AP	DF, NS, WS	RA	N/A	B	EX
Masaryk University	W, F, E, SI, MA	DF, NS	OP, RA	CR, CS	B, RD, G, YL, WT, P	EV, WS, EX
AIT Austrian Institute of Technology	W, F, E, DD, AP, R, MA	NS, WS, OS	OP, RA	SC, CR, CS, CO, IT, LG	B, RD, G, YL, WT, P	EV, WS, EX
Naval Postgraduate School	W, C, E, DD, SI, MA, RE	C, SS, NS, WS	L	Various	N/A	EI
Norwegian University of Science and Technology	W, C, F, E, S, DD, AP, R, SI, MA, RE, RM, ISE, CM, CP	C, DF, HS, SS, NS, CS, WS, CM	OP, RA	SC, NC, CR, CS, M, CV	B, RD, WT, P	EV, WS, EX
Virginia Tech	W, C, F, E, S, SI, RE	C, DF, SS, NS, WS	RA	N/A	N/A	EV, WS, EX, EI
Università degli Studi di Milano	W, F, SI, MA, RB	DF, WS	OP, RA	N/A	B, RD, G	N/A
JAMK University of Applied Sciences	W, C, F, E, S, DD, AP, R, SI, MA, RE	DF, HS, SS, NS, CS, WS	OP, RA	SC, NC, CR, CS	B, RD, G, YL, WT, P	EV, WS, EX
Swedish Defence Research Agency	W, F, DD, R, MA	SS, NS	OP, RA	SC, NC, CR	B, RD, G, WT	EV, WS, EX

Table 2.4 has the following analysis: Manual Scripting (MS), Ansible (A), Docker containers (DC), Vagrant (V), Packer (P), Openstack Heat (OH), PROXMOX (PR), Virtualbox (VB), Openstack (O), Cloudformation (CL), VXLAN (VX), Labtainers designer tool (LDT), Custom (C), Artifacts Gathered (AG), Jeopardy Board (J), CloudCTF (CC), Internal Tools (IT), JSON (JS), YAML (YM), Multiple Formats (ML), XML (X), Automatic (A), Xentop (XT), API (AP), OSSIM (OS), Snort (SN), Suricata (SU), Netflow (N), Wireshark (W) , MALCOM (M), Nagios (NG), Cloudwatch (CW), DNP3 (D), Bespoke (B), OpenFlow (OF), GHOSTS (G), AutoIT (AI), Bot(BT), Yes (Y), and Not Available (N/A).

The motivation for the questionnaire was, despite a large number of published works and surveys [16–20], the lack of data on the tools used for the development and management of CRs, when used to organize cybersecurity exercises and provide a data-set for further research. At first, it was checked to see if there are CR systems in universities and research centers in Greece. The limited number of existing systems that are located in Greece led us to broaden the search in Europe, Asia, and the rest of the world.

The questionnaire was addressed to technical directors or managers who were directly involved with the CR. The survey was conducted between June and August 2020.

The results of the research were produced by 10 different systems located in nine different countries and two continents. The countries are the USA, the United Kingdom, Italy, Norway, Sweden, Finland, the Czech Republic, Belgium and Austria.

2.3.1 Cyber Range Objectives

The first question was about the objective of the CR and, as expected, participants answered that their main objective is training.

The largest percentage of the participants use CR systems for research, training, and security exercises [18, 20]. No participant has developed a system exclusively to cover a

single objective, and, more specifically, 80% of participants cover at least two, as shown in Figure 2.1.

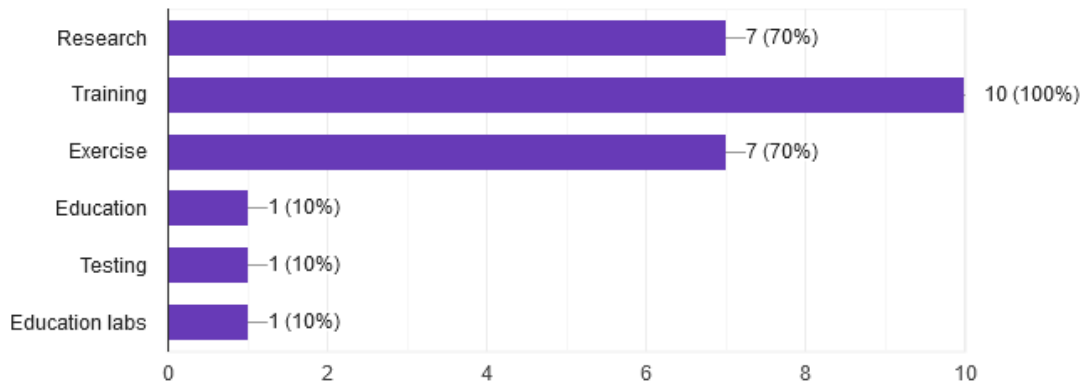


Figure 2.1 Objectives of the Cyber Range.

2.3.2 Supporting Sectors of Cyber Range

Question 2. The questionnaire was sent to the CR system providers covering all four key areas [16] Academic, Government, Military, and Private Enterprise. We have covered this requirement due to the feedback from all areas, Figure 2.2.

Of course, the majority of the answers as shown in the figure supporting sector are mainly from the Academic sector. This is because military and Private Enterprise providers do not disclose details about their systems due to confidentiality, and the existing literature is limited. However, we have managed to cover all areas, even for the military and Private Enterprise sectors, and draw useful conclusions about technologies, implementations, and development tools as shown in the next questions.

2.3.3 Domain of Cyber Range

In question 3, we have another categorization of a CR, which is the domain in which the systems operate. Another area that is flourishing is the conduct of cybersecurity exercises [68–70]. As expected, the results of the domain cybersecurity competition are very high, Figure 2.3, about 80%, as well as in SCADA, reach 60%. An interesting conclusion

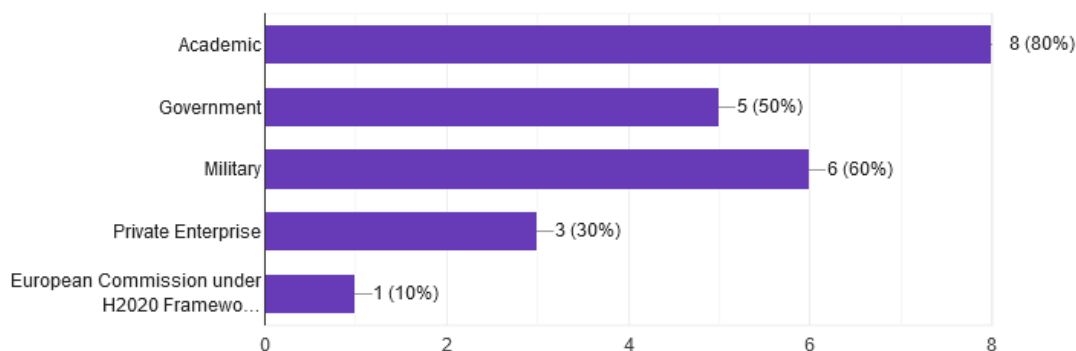


Figure 2.2 Sectors of the Cyber Range.

from the analysis of the results is that 30% of the systems are focused only on conducting security exercises, and 20% only on SCADA.

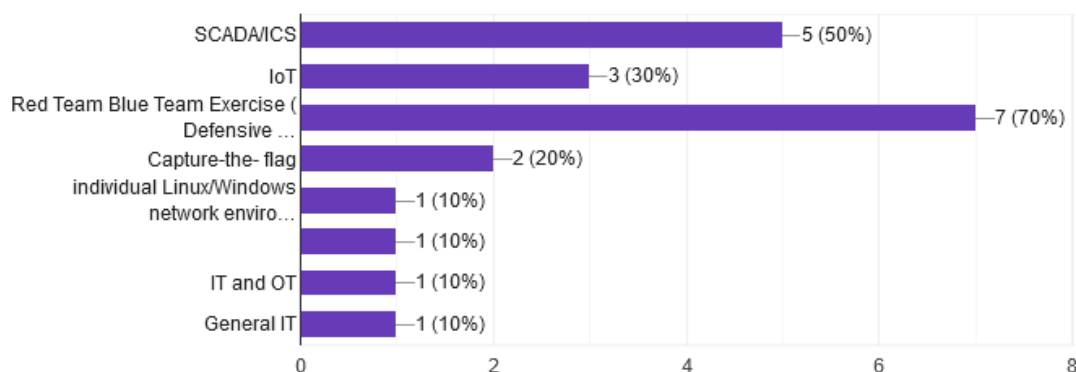


Figure 2.3 Domains of the Cyber Range.

Mainly after the incident of Iran's nuclear program, and the attack of the Ukraine power grid, a great development in CR systems aimed at improving the security of SCADA ICS and Operational Technology (OT) generally was observed. By correlating questions 3, 4, and 5, we observe that CRs do not focus only on one domain as before but have evolved by adding new components and managed to cover many domains like business, banking, telecom, health, and transport.

2.3.4 Type of security challenges

Question 4 describes the security challenges that occur in CR platforms. The most popular challenge is web security which is provided by all responders. In addition, as shown in Figure 2.4, Forensics comes first with 80%, and Exploitation and Malware analysis follows with 70%. Additionally, one of the responders stated that they can create any challenge based on specific demands.

The content of security challenges [19] varies and depends on the type of cybersecurity competition or curriculum of the university/research center. Cyber security exercises allow students to gain hands-on experiences while immersed in environments that mimic real-world operational systems. Highly realistic training allows students to gain valuable experience that employers are looking for [71]. A very interesting approach is the inclusion of challenges like Risk Management, Information Security Economics, Cyber Crisis Management, and Cyber Policy Analysis. These are hot areas and we suggest other universities to add these kinds of challenges to their CR platforms.

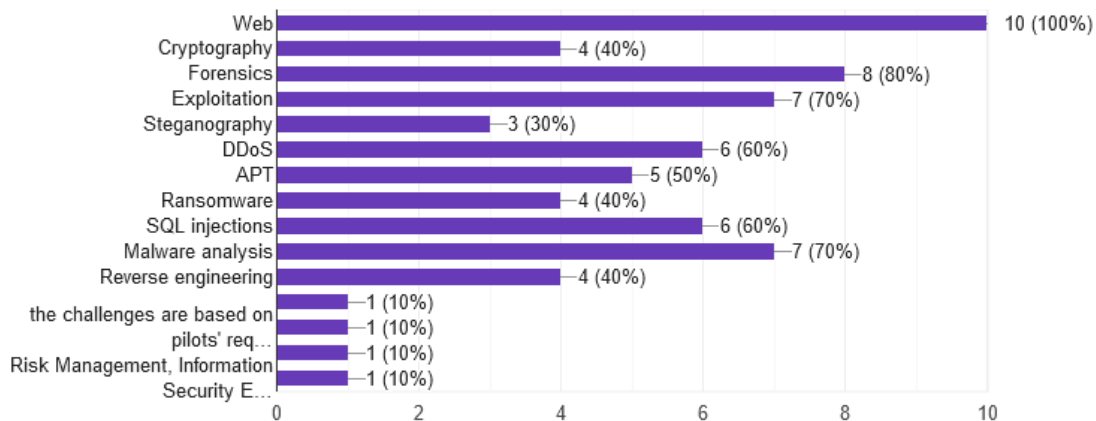


Figure 2.4 Security challenges of the Cyber Range.

2.3.5 Educational purposes of Cyber Range

A key motivation of our research is the development and implementation of a CR platform for the University of West Attica that covers three areas of research, education, and conducting

security exercises. To better address the educational aspect, aimed to determine whether the CR platform is also utilized for educational purposes. All responders answered positively. According to Beveridge [71], injecting realism into cybersecurity training and education is beneficial to rapidly train qualified, skilled, and experienced cybersecurity professionals. Additionally, we asked which courses they use for the CR platform. The most popular courses as shown in Figure 2.5 are network security by 80%, followed by web security and digital forensics by 70%, and software security by 60%.

Universities are linked to the educational curriculum courses related to emerging technologies such as cloud security, OT security, and Data-driven cybersecurity management. Cyber Ranges can combine security courses and hands-on experience and give cybersecurity experts the mentality, problem-solving capability, and appropriate technical tools for capacity building.

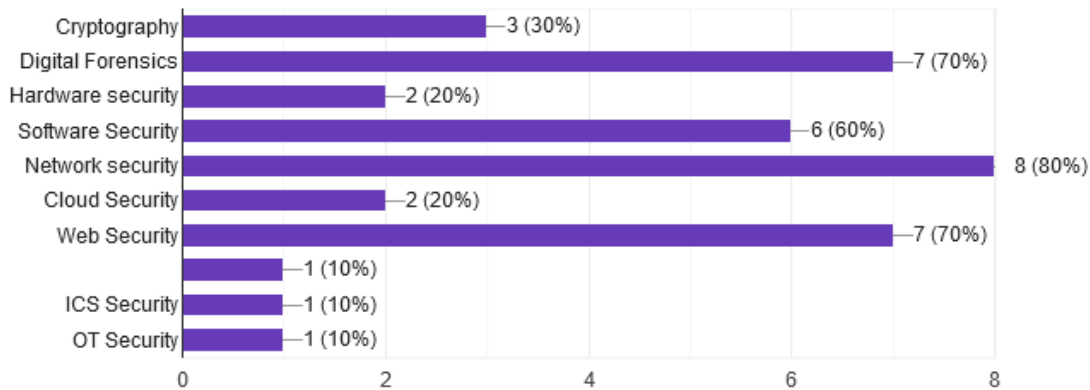


Figure 2.5 Educational courses of the Cyber Range.

2.3.6 Type of environment

Another categorization of CRs is the type of environment. Davis [16] in 2013 categorize CR and security testbeds in three main categories emulation, simulation, and Ad-hoc or Overlay. In our questionnaire, we asked the participants to identify the environment also in three categories—the first is emulation: a testbed built with real hardware or software, the second is a simulation: a testbed built with software virtualization, and the last is Hybrid/Cyber-

Physical: virtual testbeds connected with real hardware. Apart from one participant who had developed an emulated environment and two participants who had developed a simulation environment, all responders have chosen a mixed type of environment, as shown in Figure 2.6.

The rapid virtualization growth helps create complex environments, thus managing to achieve the highest possible accuracy, fidelity, scalability, and flexibility while reducing implementation costs. Additionally, by using a simulation/hybrid environment, a university can develop a CR [72, 73, 40, 74], while, before 2010, CR was developed for military purposes only (Emulab [75], NCR, StealthNet, and LARIAT [76]) mainly due to high development and maintenance costs.

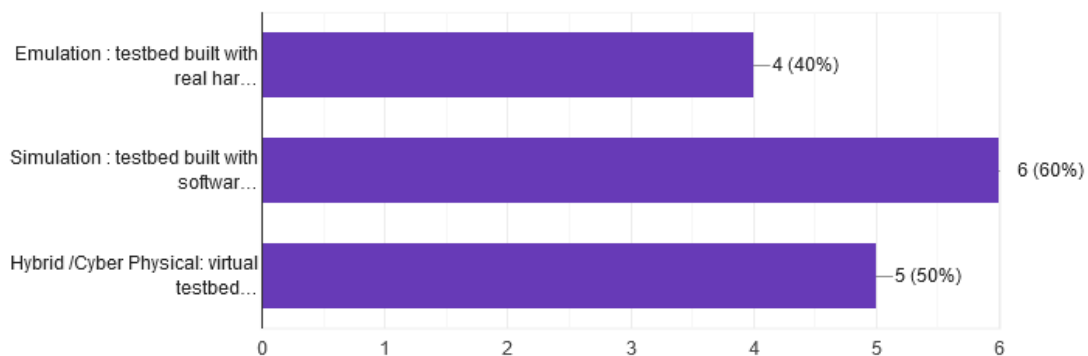


Figure 2.6 Types of environment.

2.3.7 Infrastructure platform

In question 7, we discuss which type of virtualization technology is chosen for the development of CR, and, according to ECSO [77], there are two types, conventional and cloud virtualization. Conventional virtualization uses hypervisor-based technology and containers, mostly Docker. A list of both types of hypervisors contains Virtualbox, Vmware, XenServer, Hyper-V, QEMU, etc. Cloud virtualization is divided into three types, public, private, and hybrid. The best advance of the cloud is the sharing of resources, great capabilities for automation and minimization of cost reduction [34]. OpenNebula, CloudStack, and OpenStack [32] are mostly used to deploy cloud virtualization [26–28]. The finding of questionnaires, as shown in Figure 2.7, says that up 50% use the cloud, both OpenStack and AWS, and 40%

use traditional technology. In addition, we conclude that OpenStack is the main tool (44%) used to deploy cloud infrastructure.

The development of cloud computing has opened new horizons for the evolution of CRs. Cloud environments constitute internet-based platforms to be used for computer technology. The technology used to develop the CR platforms is mainly open source and the use of commercial tools is partial. We found that the use of container technology has little impact on the systems we analyzed. We believe that there should be greater development through container technology since it improves realism and user behaviour [14].

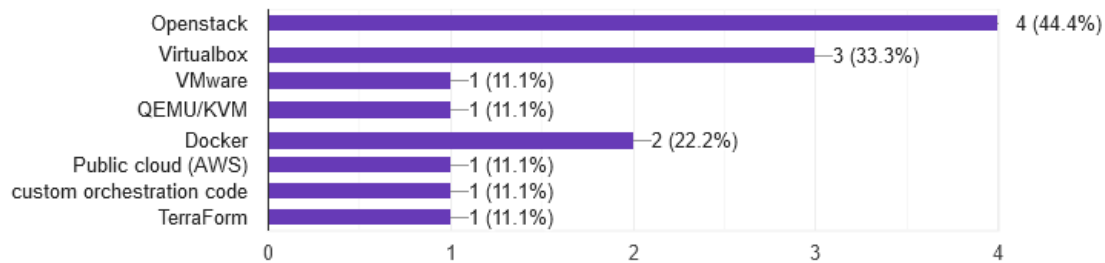


Figure 2.7 Infrastructure platform.

2.3.8 Type of access

Question 8 is about the type of access that CRs can provide to platform participants. As presented in Figure 2.8, these are on-premises 70%, remote access 80% and 10% local. Moreover, 60% of CRs can provide both types of access, on-premises and remote access. In addition, finally, one platform can provide only on-premises access. The advantage [71] of providing remote access to participants is important for conducting distance learning courses, or long-distance security competitions.

2.3.9 Implementation tools

Question 9 is one of the most important questions we asked in the questionnaire. When searching in the literature to find out how to implement a CR system, the result was disappointing and the findings were negligible, especially regarding military and commercial

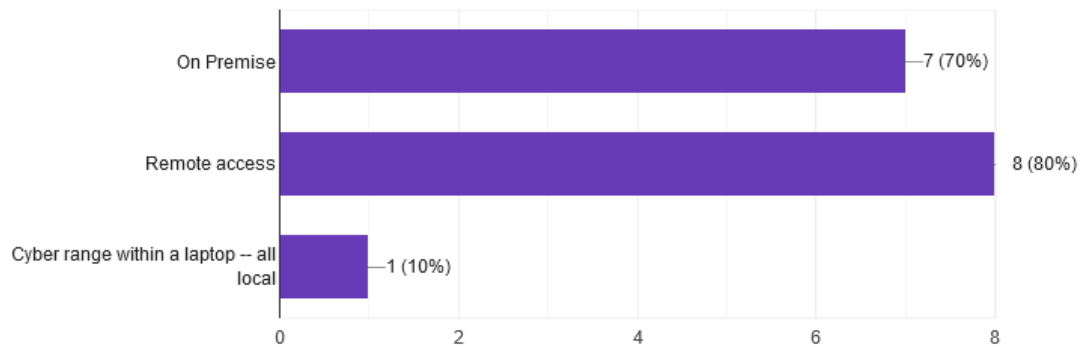


Figure 2.8 Type of access.

systems. With the main motivation of discovering the design technology and the implementation tools, we proceeded to compile this question. As shown in Figure 2.9, the technology of CRs is dominated by the use of Infrastructure as code (IaC) tools [32–35] and especially Ansible with 40%, Vagrant, and Packer. In addition, in a small percentage, where there is no cloud infrastructure, the configuration of virtual machines is done with the use of manual scripting with an imprint on the speed of implementation and the flexibility of configuration.

Today, IaC is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. IaC tools are used to configure systems, deploy software and updates, and orchestrate. The biggest advantage is the speed and ease of their use as opposed to manual scripting.

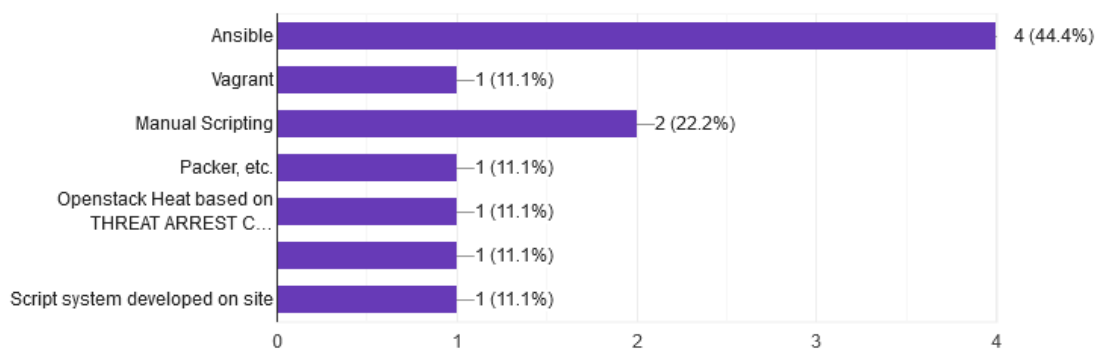


Figure 2.9 Set up VMs.

The tools used for the network topology are shown in Figure 2.10. Network tools provided by the infrastructure platform are mainly used. This can guide researchers/developers to invest in network tools that can be adopted by other CR systems.

To keep scoring during cybersecurity competitions like cyber security exercises or CTFs, several tools and mechanisms are provided. These tools are responsible for counting the flags in CTF [19] and awarding points, or artifacts from a CDX. As shown in Figure 2.11, the majority of scoring tools are custom-made and depend on the challenge, the architecture of exercises, and infrastructure platforms.

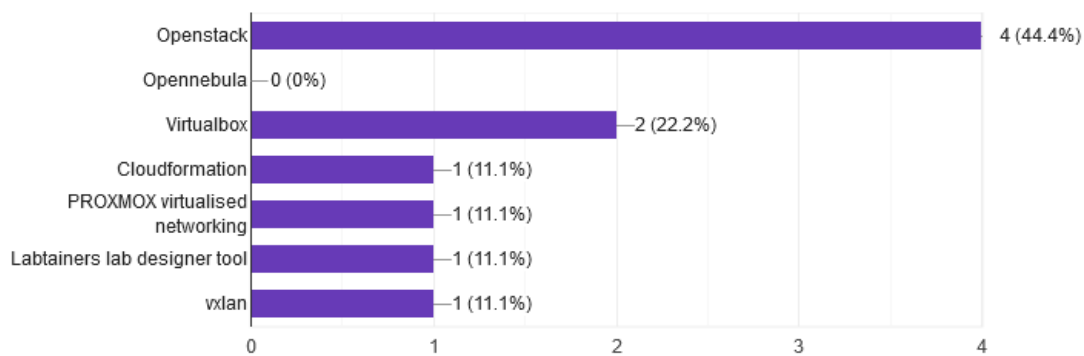


Figure 2.10 Network topology.

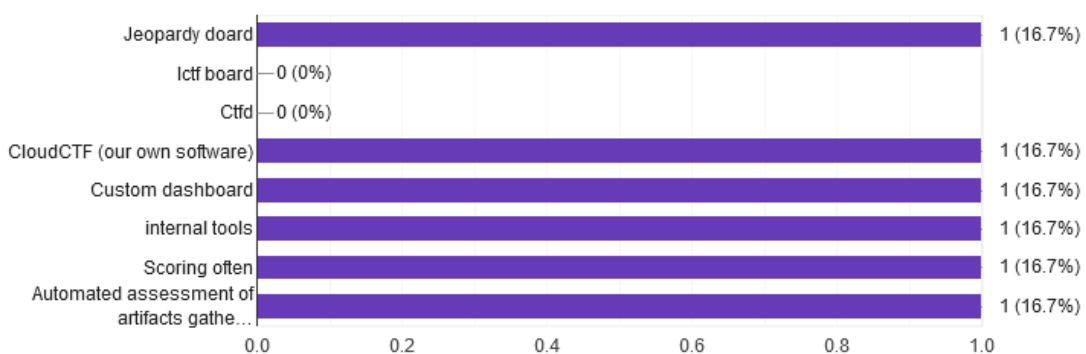


Figure 2.11 Scoring tools for Cyber Ranges.

JSON and YAML are the main scripting languages used as shown in Figure 2.12, for designing a CTF or CDX. In addition, with the use of scripting language, it became possible to create dynamic scenarios. Planning an exercise requires a script. The scenario was initially static and required the configuration of all parameters during the development of each

exercise. This resulted in complex development and management of exercises, required high management costs, and demanded long development times recently, with the development of dynamic scripts [9, 78] based on scripting languages such as JSON, YAML, and XML or IaC [35] Tools.

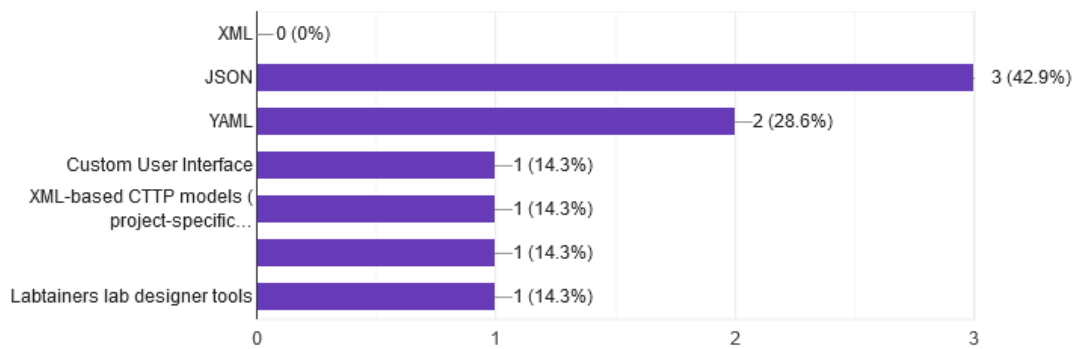


Figure 2.12 Tools to create cyber security scenarios.

A CR platform should have the right tools for managing users and groups as shown in Figure 2.13. Moreover, the CR must have a graphical user interface (GUI), capable of managing resources [33] like memory, usage, performance, reports, error logs, alert, etc. The responders identified that most use tools that are provided by the platform (OpenStack, Proxmox, AWS) or developed their own tools.

Dynamic scenarios require minimal administrative effort and in less time (from seconds to a few minutes) that could include new environments with different network topologies. This may be an opportunity for researchers/developers to produce tools that can be used by other systems.

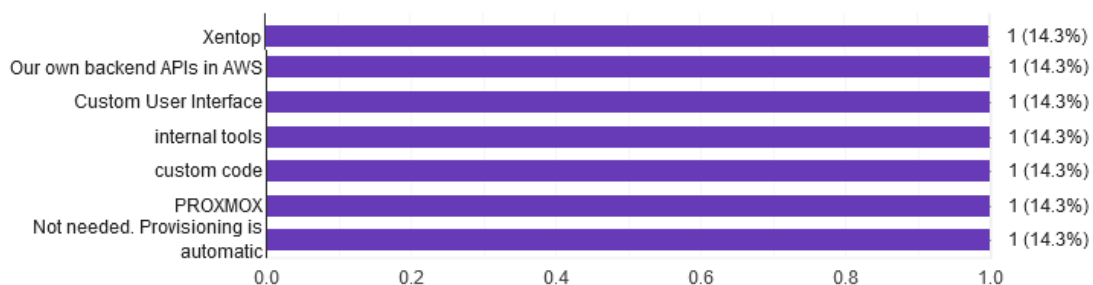


Figure 2.13 Tools to manage.

The CR platform must be able to monitor data. It must have all the necessary components for supervision, whether they are exercise training, research, or testing a system. The tools deploy depending on the type of exercise or field of the research. The responders answered that they are mostly used for monitoring purposes and open-source tools (see Figure 2.14), mainly SIEM tools such as OSSIM or Nagios. IDS tools such as Snort or Suricata are also used.

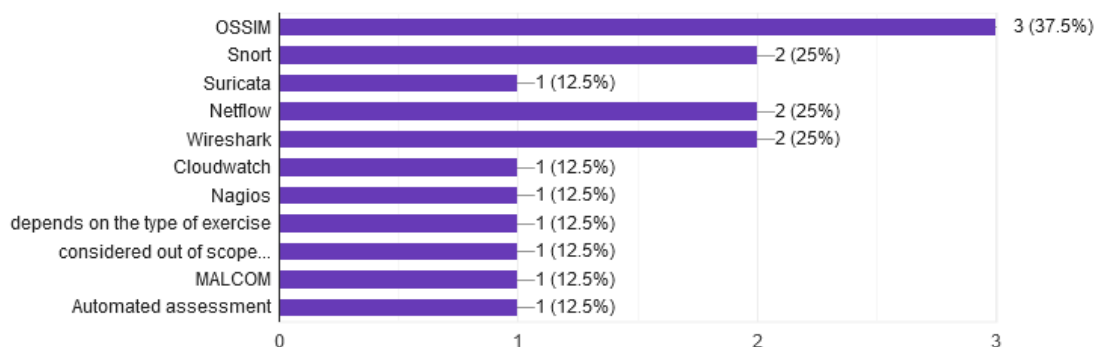


Figure 2.14 Tools to monitor.

CR platforms use tools [79–81] for monitoring data. OpenFlow and DNP3 have been used by the responders in several occasions, but mainly in-house tools or scripts are used, as shown in Figure 2.15. Testing of security tools [82] should take place under conditions that are as realistic as possible. Network traffic of the testing infrastructure should approach a real network of a company or a university [83]. Based on the answers, we don't find a tool that has a high level of acceptance yet.

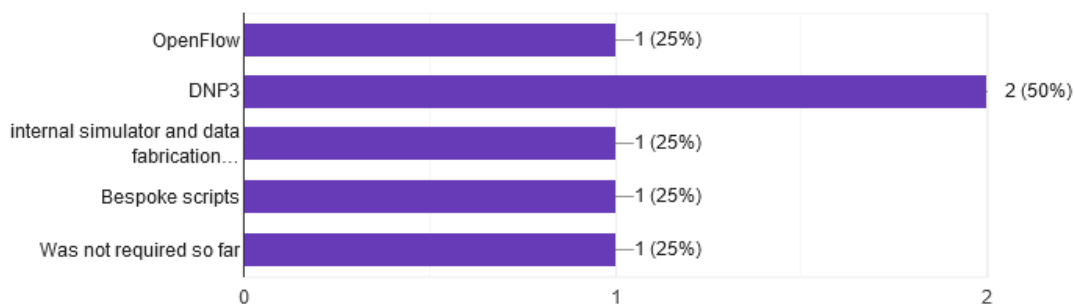


Figure 2.15 Network traffic.

Another example of an automation user/team is the automation of the red team in conducting cybersecurity attacks. The use of such an automated team covers the need to find qualified cybersecurity experts with knowledge on attacking systems, which is very difficult. There are published papers describing how to create such red teams mostly in the military domain such as K0ala from Lincoln Laboratory [76] and SVED from FOI [54] that were used for automating the behavior of a red team. GHOSTS as shown in Figure 2.16, a tool developed by the SEI, creates non-player characters (NPCs) that behave realistically without human intervention to help build complex cyber simulations. GHOSTS creates NPCs that behave like real people to generate context-driven traffic. As a result, creators of simulations can challenge participants in blue or red teams with engaging content that helps them develop elite skill sets [14, 84] and red team automation. From the answers, we notice that systems have used the GHOSTS tool [14] that develops SEI and provides through GITHUB, while the other platforms have developed their own tools.

In general, scripting languages are capable of creating complex environments, including realistic user behavior, thus improving realism. In such a use case scenario, an automated user can send or receive emails, browse the internet site, open office documents or print them, etc., resembling a typical office user who works in a company working environment. Realistic user behavior is an important part of creating complex cybersecurity exercises.

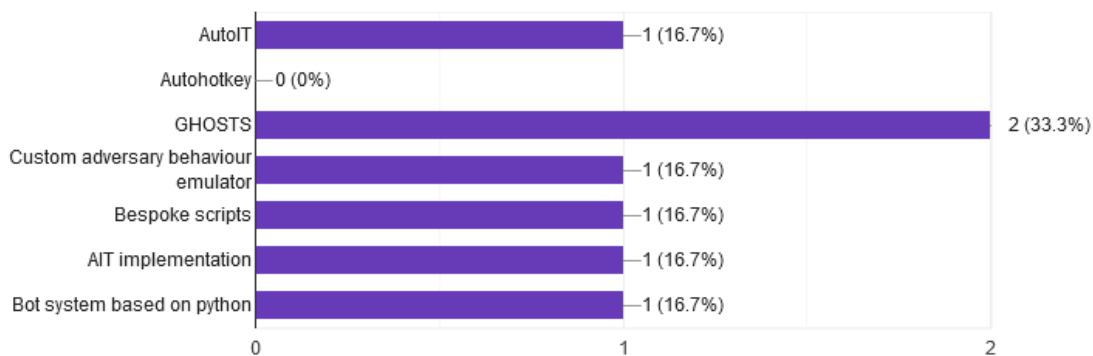


Figure 2.16 User behavior.

2.3.10 Teams, Roles, and Participants

In question 10, we identify how many groups can participate in an exercise. The answers were quite different and related not only to the implementation of the CR but also to the capacity of the infrastructure of the environment that supports it. The answers varied from systems that support only groups with one user to systems with a capacity of thousands of groups. However, on average, systems support up to 10 groups. Moreover, we examined the total number of participants which varies from one to thousands of simultaneous users. The average of users falls in the range between 50 and 100. Another point of measurement of the analysis and complexity of the exercises [85] is the number of different teams [18] that participate. As expected, the teams [86] that mainly participate are the blue 80% and the red 70%. In addition, apart from two participants who did not inform us about the teams, at least half of the participants stated that blue, red, yellow, purple, green, and white teams take part in the exercises as shown in Figure 2.18.

One main purpose of question 10 was also to identify the complexity of the exercises and the capacity of the CRs. The roles of the participants are also very important, since they support, as shown in Figure 2.17, the development of security teams such as SOC, NOC, CERT, and CSIRT. It is also interesting that, in some cases, some other roles were used by CRs such as Managers, C-level executives, and legal representatives.

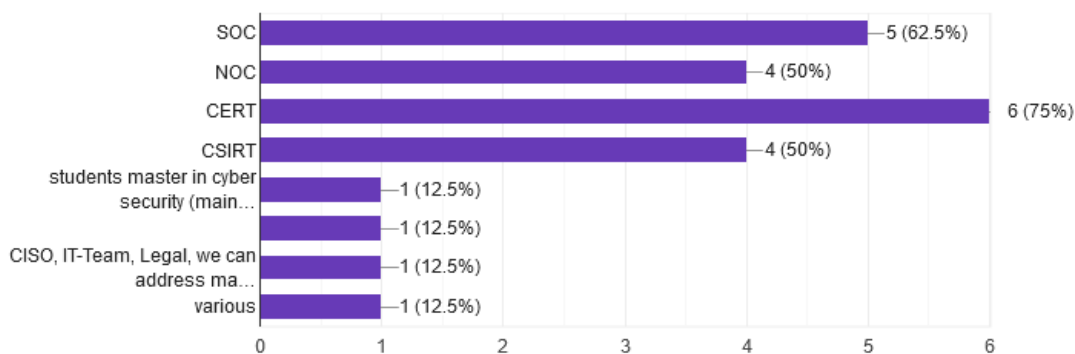


Figure 2.17 Roles of participants.

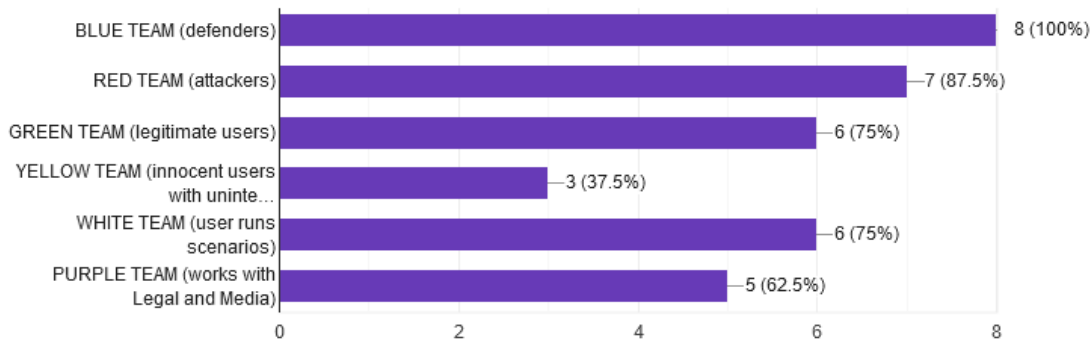


Figure 2.18 Cyber Security Teams.

2.3.11 Prior Usage of the Cyber Range

In question 11, we asked the participants if the CR platform had already been used. As shown in Figure 2.19, 90% of the respondents answered positively. In many cases, a system is created for research purposes, such as a research program that has an expiration date. The CR systems analyzed in this questionnaire are already used for educational, research, or CDX and presented in a public event.

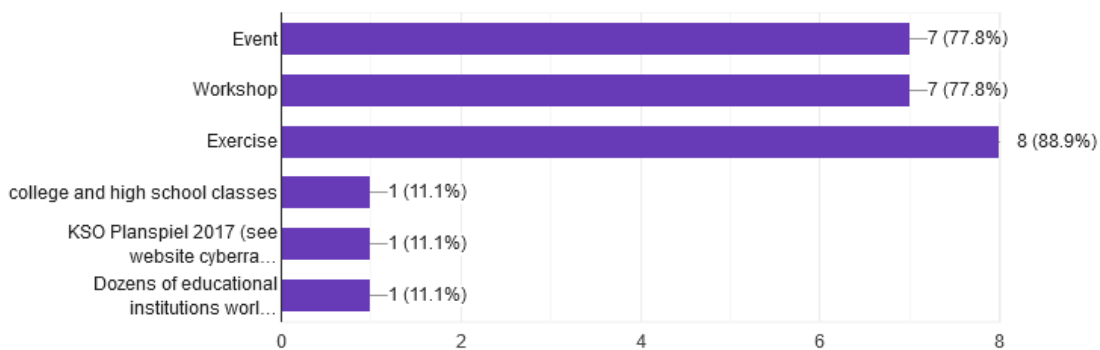


Figure 2.19 What type of event.

2.3.12 Availability of Datasets

The last question is about datasets. An important element of datasets is whether they contain measurable data. Researchers using datasets can evaluate the performance of IDSs, measuring their accuracy, false positives, and overall efficiency. In Figure 2.20, the results showed that

a large percentage, around 60%, of the systems produce datasets or this action is included in the upcoming plans.

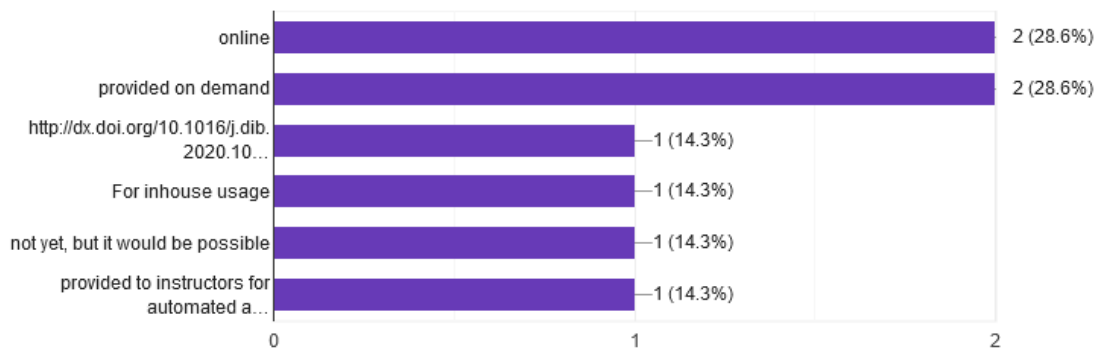


Figure 2.20 Dataset.

The creation of a dataset that contains captured network traces, from cybersecurity exercises, can enhance or produce new sophisticated methods of detection techniques for cybersecurity attacks (see Figure 2.21).

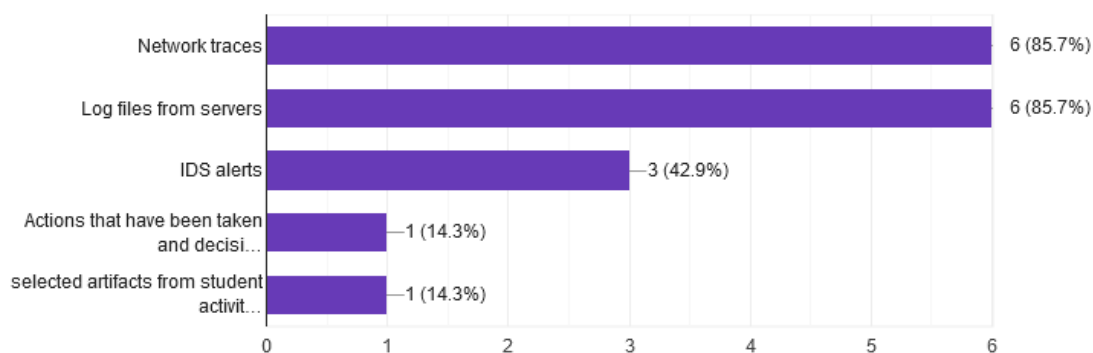


Figure 2.21 Dataset.

2.4 Challenges and Future Directions

CR research teams should be focusing on improving various aspects of their testbeds. In addition, modern CRs should be enriched with novel features, such as various telecommunication capabilities, emulated Banking systems, hospitals [87], simulated smart grids, automated

vehicles [88], Virtual Cyber Centres of Operation, wireless sensor networks, real-time Intrusion Detection Systems [89], honeypots [90], novel authentication mechanisms [91], mobile security scenarios, and several privacy mechanisms. By adding these features, new attack scenarios can be easily deployed on a testbed, revealing vulnerabilities of the various systems and thus allowing the researchers to develop innovative defense mechanisms. Moreover, any novel CR should be built in a way that could be easily used for research purposes inside EU projects. This could be accomplished if the CRs are capable of being connected to various real-world devices in the network, making it that way ideal for launching attacks and testing the defense mechanisms of various systems. One other important aspect that should be taken into account is the capability of modern CRs to create measurable data in a semi-automated way with limited human intervention.

Modern CRs should include a portable version for demonstration purposes and for easy deployment as a modern teaching instrument in various cyber security events that take place around Europe. Moreover, research teams should also be working towards the capability of their CRs to provide remote access to researchers. Via such a federated model, researchers all around the world will be allowed to implement various protocols and study their behavior in custom tailor-made environments. Finally, the need to move from traditional CRs to digital twins is a trend that is going to become dominant soon, especially for replicating critical infrastructures.

2.5 Conclusions

In this chapter, a systematic survey of ten CRs with a structured interview are presented. The purpose of the questionnaire are to examine key components that consist of a CR platform, particularly the tools used to design, create, implement, and operate a CR platform. As analyzed in Section Analysis of Results, most of the current CRs are moving towards more realistic and competitive scenarios that can help users receive focused experiential learning. The combination of emulated and simulated into hybrid environments can help a CR to be more adaptive, expandable, and thus efficient.

Chapter 3

Cyber Range Design

This chapter focuses on the proposed architecture for the Cyber Range system. Beginning with the delineation of requirements and specifications, it progresses to describe the architecture in detail. The goal is to outline a comprehensive and robust design that addresses the limitations identified in the existing systems, ensuring scalability, adaptability, and seamless integration.

A thorough understanding of the proposed architecture's structure and functionality is provided, mapping specifications to the requirements for effective cybersecurity training and research. The design incorporates advanced features to simulate a wide array of cyber threats and responses, creating a realistic and immersive environment for learners and researchers.

By laying out the foundational design elements, this section sets the stage for the subsequent implementation and evaluation of the Cyber Range system. The focus is on creating a flexible and efficient architecture that can support diverse cybersecurity scenarios and training needs.

Recent proposals for cyber range designs reflect the growing complexity and necessity of realistic environments for cybersecurity training and research. Cyber ranges are critical for developing, testing, and validating security measures in a controlled setting, allowing for the simulation of cyber-attacks and defense mechanisms. The architectural components of these cyber ranges vary, tailored to meet specific objectives such as flexibility, scalability, and realistic simulation of cyber threats.

Yamin [18] proposed eight key components: Portal, Management, Training and Education, Testing, Scenario, Run-time Environment, Logging, and Evaluation. The Portal serves as the interface for communication between the cyber range and its users, allowing for scenario creation and resource management. The Management component handles resource allocation and role assignments. The Training and Education module provides cybersecurity training with a scoring mechanism for evaluation. The Testing component conducts security assessments and system evaluations. The Scenario module enables the creation, deployment, and execution of cybersecurity scenarios. The Run-time Environment supports the operational execution of these scenarios. Logging collects extensive data for analysis, and Evaluation uses this data to assess and improve the cyber range's performance. Sharifi et al. [92] propose CyberIoT a Cyber Range for IoT that focuses on infrastructure provisioning and sandbox management to support IoT security training. The modules are, the infrastructure provisioning and sandbox management, data store, monitoring module, and web portal. Low [93] proposes an architecture of the Industrial Control Cyber Range System comprising seven modules: the Controller, Virtual OS, Web Application, Database, Exploit, Defend, and Visualization modules. Vykopal et al. [37] introduced KYPO Cyber Range which is designed as a modular, cloud-based system with five main components. The Infrastructure Management Driver controls the raw computing resources, managing virtual machines and networks through a unified API. The Sandbox Management Component orchestrates the creation and configuration of sandboxes using advanced networking techniques. The Sandbox Data Store manages sandbox-related data, bridging configurations between the cloud infrastructure and virtual machines. The Monitoring Management Component provides detailed control over monitoring configurations and exposes data to external consumers. Finally, the Platform Management Portal serves as the primary user interface, facilitating interaction with the Cyber Range throughout the sandbox lifecycle.

In a systematic review [94] we identified the state-of-the-art Cyber Ranges and testbeds used for training, education, and research purposes. These platforms employ a variety of virtualization technologies, design considerations, and complex cybersecurity scenarios to deliver dynamic and intricate environments. However, the lack of a Cyber Range that is

cloud-based, open-source, network-isolated, flexible, scalable, requires minimal resources, can conduct cybersecurity exercises, and can be developed at low costs using modern Infrastructure as Code (IaC) tools is a key motivation for our research.

In this chapter, we propose an architecture design for the Cyber Range platform and a flexible mechanism to design complex topology.

3.1 Cyber Range Architecture Model

ETHACA Cyber Range architecture involves leveraging powerful capabilities for cloud infrastructure management, combined with efficient deployment and management. Each module of the ETHACA Cyber Range benefits from the modular, scalable, and flexible architecture. Below, we delve into the architectural design of each module within this context, focusing on how they integrate and function within the broader Cyber Range environment.

The ETHACA Cyber Range architecture consists of six modules, the *Web Fronted*, the *Storage*, the *Scenario*, the *Management*, the *Environment*, and the *Orchestration* module, as illustrated in Figure 2.13. In the following paragraphs, descriptions of the modules introduce their functioning and interoperability.

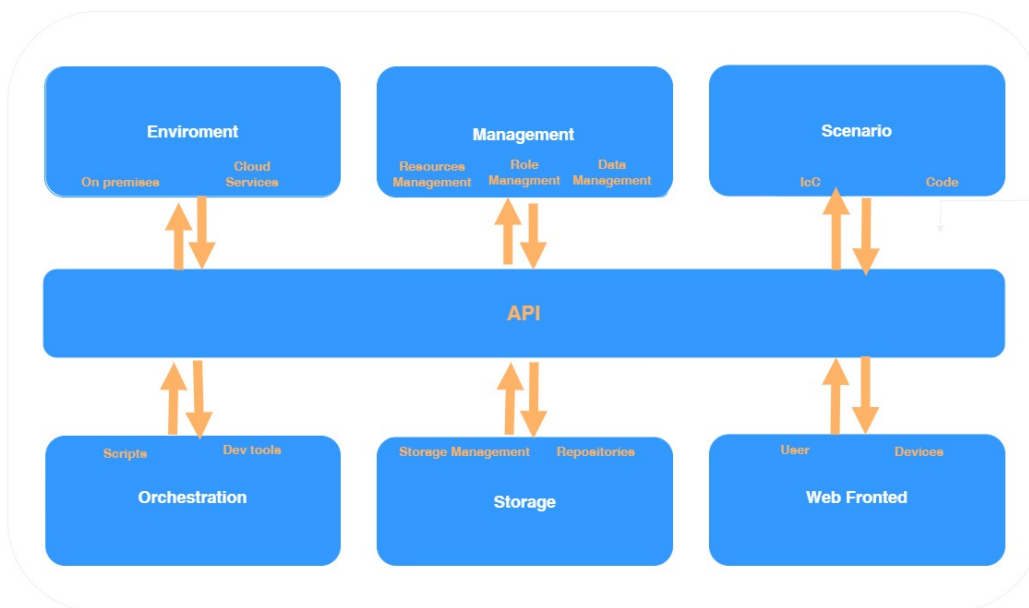


Figure 3.1 ETHACA Cyber Range Architecture.

3.1.1 Web fronted

The Web Fronted module acts as the essential gateway for users into the Cyber Range environment, enabling interaction with a wide array of services including computing, networking, storage, and orchestration, alongside scenario generation and management capabilities. This module harnesses the Horizon dashboard, enriched through bespoke web services, to cater specifically to the nuanced demands of Cyber Range activities.

Dashboard Customization: The Web Fronted module undergoes significant modifications to incorporate features crucial for Cyber Range operations. These enhancements facilitate scenario deployment, resource allocation, and comprehensive access management.

Cyber Range Service Integration: The Fronted module connects with pivotal services such as compute, network, and storage. This integration extends to specialized scenario and orchestration services devised for the Cyber Range, ensuring an intuitive user experience.

Enhanced Security through Access Management: Employing identity framework, the module delivers stringent access controls and management protocols. This ensures users are granted permissions precisely aligned with their roles in Cyber Range exercises, bolstering security.

Dynamic Scenario Deployment: Leveraging an orchestration tool, the module empowers users to dynamically deploy and manage intricate scenarios directly from the web interface. These scenarios are meticulously crafted using Heat templates that detail the necessary resources and configurations for each exercise.

Monitoring and Visualization Support: Integral to the module, though operating in the backdrop, are advanced monitoring and visualization tools. A real-time monitoring system integrates into the infrastructure to track the health and performance of the Cyber Range, gathering data across various components. A complementary visualization tool provides a visual representation of these metrics through detailed dashboards. This symbiosis not only facilitates proactive infrastructure management but also enriches the user interface by preemptively identifying and addressing potential issues, thereby ensuring a fluid and uninterrupted user experience during Cyber Range exercises.

3.1.2 Storage

The Storage module is tasked with the comprehensive management of critical data such as scenario artifacts, test images, and essential operational data.

Multi-Protocol Support: By harnessing the capabilities of block storage, the module provides a flexible storage solution that caters to a variety of needs. It supports a diverse range of protocols such as LVM, iSCSI, and NFS for block storage, to meet the diverse requirements of Cyber Range scenarios. The ETHACA Cyber Range storage service is designed to support a comprehensive range of disk and container image formats, ensuring versatile and seamless integration for users. It accommodates disk image formats including raw, qcow2, ISO, and VHD, alongside container formats such as OVF and Docker. This extensive support enables users to upload and deploy a wide variety of images onto the platform, facilitating a flexible and efficient setup for various cybersecurity scenarios and exercises. By offering compatibility with these common disk and container formats, the ETHACA Cyber Range ensures that users can easily import and manage their virtual machine and containerized applications, making it an adaptable solution for cyber security training, testing, and research activities.

Image Service Enhancement: Through image storage, the module excels in the management of virtual machine and container images, broadening its support to encompass numerous disk and container formats. This extension ensures the streamlined sharing and deployment of images across the Cyber Range, bolstering operational efficiency. Image service can act as an image registry for sharing images, allowing participants to discover, retrieve, and register VM (virtual machine) images and container images.

High Availability and Scalability: The storage services are configured for high availability, safeguarding data against loss and ensuring it remains accessible even under adverse conditions. Scalability is adeptly handled, allowing for the dynamic distribution and redistribution of storage resources in alignment with the fluctuating demands of various scenarios and exercises.

Secure and Efficient Artifact Management: The module emphasizes the security of stored artifacts, implementing stringent measures to protect sensitive information. Using

snapshotting and cloning features enhances efficiency, enabling quick deployment of pre-configured images and environments for a swift operational onset.

Container Management Service (CMS): Integral to the Storage module, container management service, introduces an additional layer of efficiency in handling containerized applications and services. In the context of Cyber Range operations, CMS streamlines the provisioning and management of containerized storage services. This aspect is particularly beneficial for scenarios that necessitate isolated testing environments, offering the versatility to deploy diverse storage configurations within containerized setups, thereby elevating the module's flexibility and scalability in storage solutions.

3.1.3 Scenario

The Scenario module is responsible for the creation, deployment, execution, control, and destruction of cybersecurity scenarios. It utilizes configuration automation tools for automation and orchestration, scripting templates for resource orchestration, and integrates with containers through Container Management Service for container management, providing a powerful platform for realistic cybersecurity training and research scenarios. Automation tools, scripting language, and orchestration templates create, deploy, execute, control, and destroy scenarios. The cybersecurity scenarios can be created, designed, and saved in a file. The scenario can provide images already stored in the image repository or can be downloaded from cloud repository using container service API. The configuration file allows for the editing and modification of several aspects like network, storage, cpu, and ever more complex frameworks like CTF, and cyber threat intelligence platforms using Docker repository.

Scenario Definition and Management: Employs Ansible playbooks and Heat templates for defining and managing the lifecycle of cybersecurity scenarios. These definitions include all necessary configurations, such as network setups, storage requirements, and specific software and services to be deployed.

Containerization for Realism and Isolation: Leverages Docker, managed via container management service, to containerize individual components of scenarios. This approach

allows for the creation of isolated, reproducible environments that mimic real-world systems and threats, enhancing the educational value of exercises.

Dynamic Resource Allocation: Integrates with OpenStack's Nova and Neutron services for dynamic allocation of compute and network resources, respectively. This ensures that scenarios can be scaled up or down based on the requirements of the exercise, providing flexibility and efficiency in resource use.

Integration with Cybersecurity Tools and Platforms: Facilitates the incorporation of specialized cybersecurity tools and platforms, for capture-the-flag or threat intelligence exercises. This is achieved by containerizing these tools and managing them through the Scenario module, allowing for a comprehensive and diverse range of cybersecurity training exercises.

Realistic Network Scenarios: Container network service enables the creation of complex, realistic network scenarios by integrating container networking seamlessly with networking service enhancing the realism of cybersecurity exercises.

Containerized Scenarios: The Scenario module allows straightforward management of containerized applications and services necessary for various cybersecurity scenarios. The ability to handle containers natively in environments means scenarios can be more easily deployed, scaled, and managed, providing a flexible and efficient approach to scenario provisioning.

3.1.4 Management

In the Management module resources like memory, computational resources, roles, storage capabilities, and network resources are managed. Exercise management assigns roles as well as computational resources to the scenario and running. The allocation of a participant's roles and resources in an activity or experiment is taken into account. In an exercise or experiment, multiple scenarios can be conducted, and management deals with controlling multiple exercises or experiment scenarios in the environment. Additionally, log data can be gathered to evaluate.

The Management module oversees the allocation and management of resources within the Cyber Range, ensuring that scenarios are executed smoothly and efficiently. It handles the assignment of roles, computational resources, and the management of multiple scenarios and exercises.

Resource Allocation and Scheduling: Utilizes compute and network services for managing computational and network resources, respectively. This includes the dynamic allocation of resources to different scenarios based on predefined roles and requirements.

Exercise Management and Control: Leverages automation tools for automating the setup, execution, and teardown of exercises. This includes managing the distribution of roles among participants, setting up the necessary infrastructure, and collecting results and logs for analysis.

High Availability and Fault Tolerance: Ensures that management services are deployed in a highly available configuration, minimizing downtime and ensuring that exercises can proceed without interruption. Fault tolerance mechanisms are implemented to automatically recover from failures, ensuring the continuity of exercises.

Performance and Health Monitoring: Within the Management module, monitoring systems is employed to collect and store metrics related to resource usage, performance, and operational health from across the Cyber Range infrastructure. A visualization platform is used to create intuitive, customizable dashboards that present this data, enabling administrators to monitor the system's status and make informed decisions about resource management, scaling, and troubleshooting.

Integrating Learning Management System (LMS) into the Cyber Range's management module significantly enriches the delivery, management, and evaluation of cybersecurity training and exercises [77]. By leveraging LMS [95], the cyber range can offer structured courses, detailed scenario guides, and interactive learning tools, such as forums and workshops, to enhance participant engagement and collaboration. LMS [96]robust tracking and reporting features enable precise monitoring of participant progress and skill assessment, facilitating personalized feedback and improvement areas identification. Additionally, it supports the creation of a comprehensive resource repository, accessible remotely to participants, thereby

extending the reach of cybersecurity education. The platform's scalability ensures that it can accommodate an expanding user base, making it an essential component for delivering a dynamic, interactive, and scalable cybersecurity training experience.

3.1.5 Environment

The infrastructure on which the scenario is implemented, covering cloud, virtual, physical, and hybrid platforms, is depicted by the environment. Provisioning creates an environment that is used for exercise purposes. To make the cybersecurity exercise and environment more realistic, computational resources, user behavior characteristics, and random network traffic can be incorporated.

The Environment module provides the infrastructure for implementing scenarios, covering a range of platforms from cloud and virtual to physical and hybrid setups. It is responsible for provisioning and configuring these environments to support the diverse requirements of cybersecurity exercises.

Hybrid Infrastructure Support: Designs and implements a flexible infrastructure capable of supporting cloud, virtual, physical, and hybrid platforms. This is achieved by integrating OpenStack for cloud and virtual resources, along with direct management of physical resources where necessary.

Realistic Exercise Environments: Utilizes advanced networking configurations, managed by network service, to simulate real-world networks. This includes the creation of complex network topologies, the injection of user behavior characteristics, and the generation of random network traffic to mimic realistic cyber environments.

Dynamic Provisioning and Configuration: Utilizes orchestration to dynamically provision resources and environments based on the specific requirements of each scenario. This includes further customization and configuration of these environments to ensure they closely match the intended training or research objectives.

Security and Isolation: Implements strong security measures and isolation techniques to ensure that exercises are conducted in a controlled and safe manner. This includes the

use of security groups, firewalls, and network segmentation to protect the Cyber Range infrastructure and its users.

Enhanced Container Networking: The container networking service role in the Environment module is critical for ensuring that containerized components of the Cyber Range, such as those deployed for specific scenarios or training exercises, have seamless network connectivity. By integrating networking capabilities with Docker, it facilitates complex network setups that are essential for simulating real-world cyber environments, thereby enhancing the quality and effectiveness of cybersecurity exercises.

3.1.6 Orchestration

The orchestration module coordinates all services. Automates infrastructure lifecycle and software provision. Orchestration of infrastructure and the creation of an environment can be achieved with a single script file (template). Resources (for example network IPs, user groups, and storage) can be created using templates, or more sophisticated features like high availability, and autoscaling. Orchestration focuses on infrastructure, but the templates work well with other IaC and configuration management tools.

The Orchestration module coordinates the provisioning and management of infrastructure and software resources across the Cyber Range. It automates these processes to ensure that scenarios are deployed, executed, and terminated efficiently and reliably.

Unified Resource Management: Utilizes Heat to orchestrate the deployment of resources across the Cyber Range. This includes the creation of compute instances, networking configurations, and storage allocations based on templates that define the requirements for each scenario.

Integration with IaC Tools: Enhances the orchestration capabilities by integrating with additional Infrastructure as Code (IaC) tools. This allows for more granular control and customization of the environment and software configurations, tailoring them to the specific needs of different scenarios.

Automated Lifecycle Management: Implements automated processes for the entire lifecycle of scenarios, from deployment to teardown. This ensures that resources are efficiently

used and released when no longer needed, reducing waste and optimizing the utilization of the Cyber Range infrastructure.

Comprehensive Orchestration: The Orchestration module leverages container orchestration, ensuring that containerized applications and services are efficiently deployed and managed across the Cyber Range. container network service is used to orchestrate networking for these containers, providing them with the necessary connectivity and network services. Monitoring services play critical roles in orchestrating the monitoring and visualization of the entire infrastructure, ensuring that resources are optimally utilized, and performance issues are swiftly addressed.

The modules and technologies of the ETHACA Cyber Range significantly contribute to the architecture's ability to support complex scenarios, manage resources effectively, and provide real-time monitoring and feedback, all of which are crucial for maintaining a high-quality Cyber Range experience.

In the following paragraph we explain the workflow mechanism in the ETHACA Cyber Range architecture as illustrated in Figure 3.1.

Participants access ETHACA Cyber Range System through the Web Fronted module's graphical user interface. They log in and browse available scenarios, selecting the one they wish to participate in. Once a scenario is selected, participants can configure specific parameters such as network settings, storage requirements, and computational resources through the Web Fronted module. They can also specify any additional customization needed for the scenario. Upon confirming the configuration, the Orchestration module takes charge of provisioning the necessary infrastructure resources. It utilizes orchestration templates, such as Heat templates, to automatically create virtual machines, networks, storage volumes, and other required components. Alongside infrastructure provisioning, the Orchestration module integrates with IaC tools like Ansible. It deploys and configures the required software components, applications, and services within the provisioned infrastructure. This ensures that the Cyber Range environment is equipped with the necessary tools for the chosen scenario. Once the infrastructure and software resources are provisioned and configured, participants can start executing the scenario. They interact with the Cyber Range environment, perform

tasks, and tackle the cybersecurity challenges presented within the scenario. Throughout the scenario execution, the Management module monitors various aspects of the Cyber Range environment, including resource utilization, performance metrics, and system health. Once participants complete the scenario initiate the cleanup process, deallocating and releasing the allocated resources, including virtual machines, networks, and storage volumes. The completed scenario, along with relevant logs and data, can be archived for future analysis and research purposes. This allows administrators and researchers to review the scenario's execution, identify areas of improvement, and gain insights into participants' performance and the effectiveness of the scenario design. The Storage module acts as a repository for scenarios, allowing administrators to store and manage scenario artifacts, templates, and configurations. It also enables sharing scenarios among different Cyber Range instances or with the broader cybersecurity community, fostering collaboration and knowledge exchange. Based on the feedback, analysis, and lessons learned from executed scenarios, administrators can make enhancements and updates to the scenarios, infrastructure templates, and software configurations. This iterative process ensures continuous improvement of the Cyber Range platform and the scenarios it offers.

3.2 Conclusions

The proposed Cyber Range platform offers several advantages over existing implementations. Firstly, it provides a flexible and scalable infrastructure for creating and running cybersecurity scenarios. The use of containerization technology allows for easy creation, distribution, and management of scenarios, reducing the time and effort required to deploy and manage them. Secondly, the platform allows for the customization of scenarios to meet the specific needs of different organizations and users. The use of open-source tools like Ansible and HEAT templates, as well as the availability of various pre-built images, allows for the creation of tailored scenarios that address specific security concerns and threats. Thirdly, the platform provides a user-friendly interface for managing the scenarios and the environment, making it accessible to users with varying levels of technical expertise. This makes it an ideal tool for

cybersecurity education and training in academic institutions. Finally, the platform offers a cost-effective solution for cybersecurity education and training. The use of open-source tools and containerization technology reduces the cost of deploying and managing scenarios, making it an affordable option for small and medium-sized universities.

A novel Cyber Range architecture is proposed, emphasizing lightweight, flexibility, resource efficiency, and scalability. Furthermore, we provide implementation and technical details that demonstrate the advantages and benefits of utilizing an open-source cloud platform, with a particular focus on container-based applications.

Hence, this leads towards a modern Cyber Range system that can supplement educational courses by giving participants hands-on experience. Collectively, these benefits make the ETHACA Cyber Range a comprehensive and user-friendly platform, providing enhanced flexibility, security, and efficiency in running scenario environments compared to existing Cyber Range platforms that are implemented using Docker container technology.

By utilizing the developed ETHACA Cyber Range, which is a more sophisticated and realistic setting, the university's research objectives will be strengthened. It will also assist the University in achieving its research and educational goals by adopting a cutting-edge scalable, isolated, and realistic environment. In the past years in particular, the UNIWA cybersecurity research team (INSSec) has actively participated in cybersecurity exercises on an international and national scale, as well as, international CTF competitions with outstanding achievements. The ETHACA Cyber Range will offer great opportunities to students for practice and preparation before such competitions and will invite more students interested in gaining such experiences.

Moreover, the INSSec research team of the University of West Attica has three times organized and coordinated the Greek university's annual CTF tournament, the UNIWA CTF, in 2020, 2021, and 2022 [97]. Using the ETHACA Cyber Range platform in the upcoming years the University will be able to accommodate more demanding events with numerous participants, as the UniWACTF.

Finally, it has been under consideration the expansion to include interdisciplinary cyber-attack scenarios, like game theoretic approaches in detection engines [98] and in security policies, which will provide research options suitable for postgraduate students.

Chapter 4

Cyber Range Implementation

This chapter aims to bridge the theoretical concepts and architectural designs with real-world applications, showcasing the deployment and integration of the CR system. The detailing of the selection and setup of the infrastructure platforms and technologies essential for the CR system is provided. This includes the deployment frameworks, virtualization technologies, and integration with Monitoring, Metrics and Learning Management Systems (LMS) . The infrastructure setup ensures a robust, scalable, and flexible environment capable of supporting diverse cybersecurity training and research activities.

Following the infrastructure setup, the chapter explores the deployment process, highlighting the challenges encountered and the solutions implemented to overcome these obstacles. This section provides insights into the technical intricacies involved in bringing the CR system to life, emphasizing the importance of seamless integration with existing technological ecosystems.

Also covers the enhancement of monitoring and alerting capabilities [99] within the CR system. Tools such as Prometheus and Grafana are utilized to ensure real-time monitoring, efficient data collection, and comprehensive analytics, thereby enhancing the overall effectiveness and responsiveness of the CR system [100].

Analyses of the market for container management software and services and predicts that the adoption of this technology will become widespread. Software containers have seen tremendous growth recently and are favored by developers for their ability to build

applications once and deploy them in any computing environment, significantly enhancing enterprise agility. Estimation [101] Gartner forecasts that by 2027, more than 90% of G2000 organizations will be employing container management tools in their hybrid environments, marking a substantial rise from the less than 20% doing so in 2023.

Cyber Ranges, utilizing IaaS frameworks such as OpenStack and operating within large data centers, gain from enhanced scalability, compatibility, security, isolation, and pooled resources. Docker Containers are used on PCs, laptops, and servers and are known for their rapid deployment, flexibility, portability, and resource efficiency. Our methodology leverages the strengths of both OpenStack and Docker containerization to create a resource-efficient, flexible, and scalable Cyber Range platform. The aim is to develop a cutting-edge Cyber Range Platform using emerging technologies. Using container-based technologies not only simplifies deployment but also improves maintenance efficiency and reduces the complexity of deployment processes. Experimental evidence suggests that Docker can significantly enhance deployment procedures while simultaneously simplifying them [102].

4.1 Infrastructure Platforms and Technologies

4.1.1 Infrastructure Platforms

According to Nist [95] the implementation of a cyber range involves several features essential for its operation, aiming to bridge the cybersecurity skills gap. These features provide the foundation for a realistic and effective training and education environment. Here's a concise overview:

- **Range Learning Management System (RLMS):** Combines standard Learning Management System features with specific cyber range characteristics to manage and track training outcomes.
- **Orchestration Layer:** Integrates various technology and service components of a cyber range, playing a vital role in the effectiveness of the training environment

by coordinating the underlying infrastructure, virtualization layers, and the target infrastructure.

- **Underlying Infrastructure:** Consists of networks, servers, and storage that support the cyber range operations. This infrastructure can be physical or virtual, with many ranges opting for software-defined virtual infrastructure to improve scalability and reduce costs.
- **Virtualization Layer:** Reduces the physical footprint of the cyber range by employing virtualization technologies, which are essential for creating economically viable and scalable cyber ranges. This layer also serves as a protective barrier between potential attack vectors and the underlying infrastructure.
- **Target Infrastructure:** Simulates the environment in which students are trained, potentially replicating a student's real IT and security infrastructure. This includes profiles of commercially available servers, storage systems, applications, and firewalls.
- **Realism & Fidelity:** Essential for developing predictive operational and learning outcomes, with a balance required between cost, practicality, and reality. The level of realism influences the effectiveness of the training.
- **Access Considerations:** Address how users can access the cyber range, including location (on-premises vs. cloud-based) and sophistication (understanding the level of effort required for installation, usage, and implementation).
- **Scalability & Elasticity:** Refers to the cyber range's ability to accommodate a growing number of users and quickly expand capacity as needed. This aspect is crucial for supporting large user populations and adapting to increased demand.

In the article [94], several infrastructure platforms and technologies are discussed as foundational elements for developing and operating cyber ranges. These include both conventional virtualization technologies and cloud-based solutions. Here are the infrastructure platforms mentioned:

1. OpenStack [103]- A cloud computing platform for public and private clouds, providing an Infrastructure as a Service (IaaS) solution. It's widely used for deploying cloud infrastructure in cyber ranges due to its flexibility, scalability, and extensive community support.
2. VMware [104]- VMware offers solutions for cloud computing and platform virtualization. It's utilized in cyber ranges for creating and managing virtual machines and environments.
3. Proxmox [105]- An open-source platform for enterprise virtualization. It integrates the Proxmox Virtual Environment for managing virtual machines and containers, making it suitable for creating flexible and scalable cyber ranges.
4. Public Cloud (AWS)[106] - Amazon Web Services (AWS) represents the public cloud infrastructure for hosting, scaling, and managing cyber range environments. AWS offers extensive services that can be leveraged for cybersecurity training and research.
5. Minimega [107] - A tool mentioned in the context of creating and managing network simulations, which can be integral to the development of cyber range environments.
6. KVM (Kernel-based Virtual Machine) [106]- An open-source virtualization technology built into Linux, allowing the kernel to function as a hypervisor. It's used for managing virtual machines in a cyber range setup.
7. Virtualbox - Oracle VM VirtualBox [108] is a free and open-source hosted hypervisor for x86 virtualization, useful for running multiple operating systems simultaneously, often used in cyber range environments for its ease of use and compatibility.

In examining the characteristics delineated in the NIST Cyber Range Guide [95], the functionalities proposed by ECSO [77] alongside the conclusions of our survey [94], it becomes apparent that OpenStack is advocated as the optimal infrastructure for the conceptualization and realization of cyber ranges. This recommendation is predicated on OpenStack's inherent qualities of flexibility, scalability, and a comprehensive toolkit for orchestrating virtualized

infrastructure components. Such attributes are critical for constructing cyber ranges that are not only realistic but also efficacious for various applications ranging from educational courses to sophisticated cybersecurity competitions. Furthermore, the alignment of Open-Stack's capabilities with the technical requisites detailed in the NIST guide—encompassing scalability, elasticity, and virtualization support—underscores the platform's suitability in meeting the diverse demands of cyber range stakeholders, thereby enhancing cybersecurity education, training, and research efficacy.

4.1.2 Deployment Technologies

Infrastructure platforms lay the foundational technological environment essential for deploying advanced cyber range systems. These platforms often leverage Virtual Machines (VMs) and Docker Containers to achieve training environments. VMs [109] provide a complete simulation of the underlying hardware, allowing multiple operating system instances to run concurrently on a single physical machine, which is indispensable for creating diverse and isolated testing scenarios that mimic real-world IT infrastructure complexities.

Docker Containers complement this by offering a more lightweight solution; they encapsulate the application layer and share the host system kernel. This arrangement is highly beneficial for cyber ranges as it significantly reduces overhead, boosts start-up times, and enhances the portability of scenarios across different environments without the baggage of entire OS instances that VMs typically entail. The transition from broad infrastructure platforms to these specific technologies illustrates a move towards more granular, efficient, and sophisticated cyber training capabilities. Lingayat et. al. [110] and Yadal et. al. [111] compare the performance of Docker and VMs in terms of computing, storage, and memory, and the results show that Docker performs better in terms of execution times for the requests and startup time at least fifty percent higher. The Virtual Machine's architecture in conceptual contrast to Docker architecture is depicted in Figure 4.1. Details on both architectures follow in the sequel.

A technology known as containerization organizes system libraries, networks, applications, and other components into a container structure. The programs are developed,

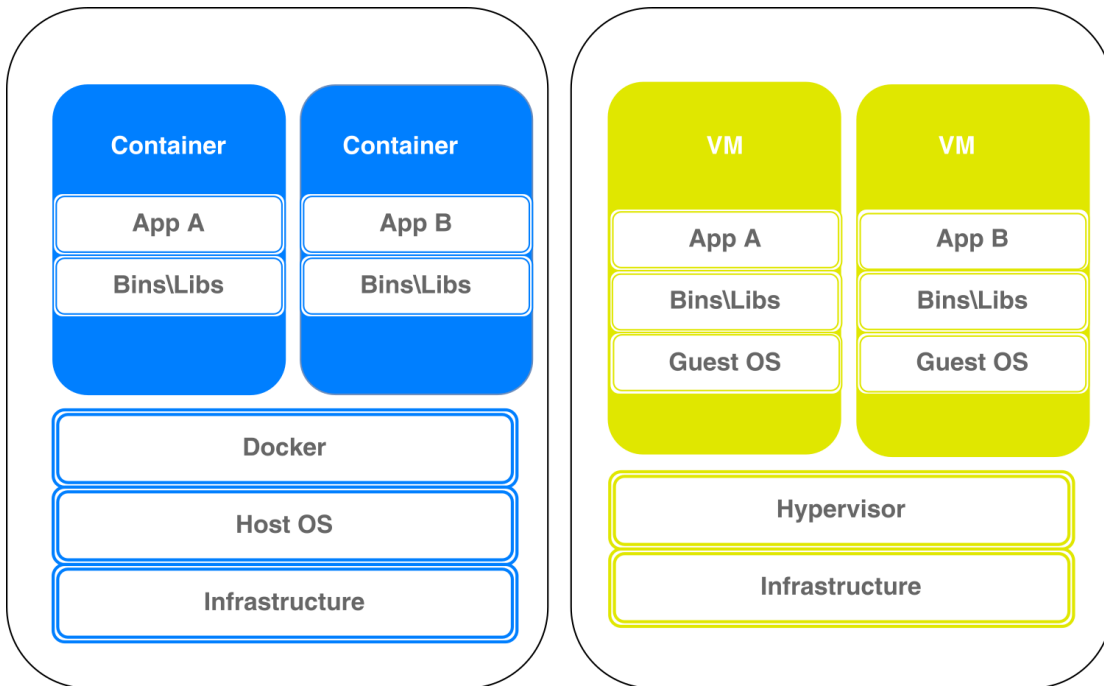


Figure 4.1 Docker vs Virtual Machine Architecture.

organized, run, and delivered in containers. Docker container [112] is a lightweight virtualization solution that ensures that the program functions in all environments and also automates the deployment of apps into containers. The container environment in which the programs are run and virtualized is supplemented by an additional layer of deployment engine.

Docker container assists in offering a speedy and light environment for code execution. Docker is based on an open-source container platform. Docker stores, shares, and exchanges in public repositories [hub.Docker.com](https://hub.docker.com), GitHub, etc, but also can upload in local and private repositories.

One of the benefits of using Docker containers is that applications are easily migrated to various machines and environments, which enhances development speed. Collaboration on complex projects is also facilitated by the ability to isolate project components into containers and evaluate them separately. Applications and services are scalable on-demand and in real-time, which significantly lowers IT costs. Finally, Docker provides simple commands to

operate virtual devices. The main reason for Docker popularity is the simple commands and the reliability of the operation.

A virtual machine VM is a computer file, software program, or image that is built inside of a host computing system. A VM is perfect for testing other operating systems, developing operating systems, and running apps and software since it can perform tasks, like executing programs and applications on a separate computer. VMs give users access to a full operating system that can run a variety of software applications.

4.1.3 Deployment Frameworks

The deployment of Virtual Machines and Docker Containers [113] within Cyber Ranges is intricately tied to the use of sophisticated deployment frameworks. These frameworks, designed for orchestrating both containers and virtual machines, facilitate the management, scaling, and networking of virtual instances across the cyber range's computing resources.

Such deployment frameworks enhance the process of scenario provisioning and management, providing tools to automate the deployment, scaling, and operation of containerized and virtualized applications. This automation is crucial for replicating complex cyber-attack scenarios and defensive maneuvers in a controlled, repeatable, and safe environment. By using these frameworks, cyber range exercises can accurately mirror real-world digital infrastructures and dynamically adapt to new threats and technologies, thereby maintaining the relevance and effectiveness of cybersecurity training programs.

In summary, OpenStack's open-source nature, flexibility, scalability, comprehensive service offerings, cost-effectiveness, customizability, wide adoption, and security features make it a compelling choice for the implementation of cyber ranges aimed at education, training, and cybersecurity research.

OpenStack, the widely used open-source cloud computing platform, provides various deployment frameworks to automate and manage the lifecycle of cloud infrastructure [114]. Each of these frameworks has its unique characteristics, advantages, and use cases. Here are the deployment frameworks mentioned:

- OpenStack-Helm aims to deploy OpenStack services in Kubernetes clusters using Helm charts. It provides fine-grained control over OpenStack deployments and configurations, making it ideal for users looking for the scalability and orchestration capabilities of Kubernetes. It's particularly suited to environments where Kubernetes is already being used or considered for the orchestration of containerized applications.
- Kayobe extends Kolla-Ansible to automate the deployment of containerized OpenStack to bare metal using Ansible and OpenStack Ironic. Kayobe focuses on the physical infrastructure layer, making it ideal for deployments where direct control over physical servers is needed, alongside the operational benefits of containerized OpenStack services.
- OpenStack-Ansible utilizes Ansible playbooks for deploying OpenStack on virtual machines or bare metal. It emphasizes a highly flexible and customizable deployment, targeting users who need intricate control over their OpenStack configuration. It's designed for operational simplicity and scalability, supporting large, multi-site installations.
- OpenStack-Charms is designed for model-driven cloud operations using Juju, a Charms collection for deploying and managing applications across various cloud services. It's especially effective for dynamic environments and multi-cloud strategies, offering an easy way to scale out services based on demand.
- Bifrost is an Ansible-based toolkit for deploying OpenStack on bare metal. Unlike other frameworks that focus on full cloud environments, Bifrost specializes in standalone, non-clustered bare metal provisioning, suited for deploying individual servers or for initial provisioning scenarios.
- OpenStack-Chef: employs Chef cookbooks for the deployment and management of OpenStack clouds. It caters to users who prefer Chef as their automation tool, allowing for customizable and automated cloud infrastructure management. This approach is fitting for organizations already invested in Chef for configuration management.

- Kolla-Ansible leverages Ansible playbooks to deploy OpenStack in Docker containers, simplifying the deployment and upgrade processes. Its primary advantage is the combination of Ansible's simplicity and the isolation provided by containerization, facilitating easier version management and system maintenance. Kolla-Ansible is well-suited for operators looking for straightforward deployment, scalability, and easy upgrade paths.

Selecting the right deployment framework depends on specific project requirements, existing infrastructure, and operational preferences. Kolla-Ansible [115], [116],[74] stands out for several reasons:

- **Simplicity and Ease of Use:** Kolla-Ansible combines Ansible's ease of use with Docker's containerization to streamline deployment and management tasks.
- **Scalability and Flexibility:** The use of Docker containers allows for easy scaling and updates of OpenStack services without impacting the entire system.
- **Operational Efficiency:** It offers efficient operations with minimal downtime during upgrades and maintenance, a critical factor for production environments.
- **Community and Support:** As part of the broader OpenStack project, Kolla-Ansible benefits from strong community support and continuous development.
- **Utilizes containerization to provide robust isolation,** ensuring that each component of the OpenStack services it deploys operates within its own secure, self-contained environment.

To significantly enhance the flexibility, efficiency, and performance of your cloud infrastructure, Zun and Kuryr are implementing with Kolla-Ansible for our OpenStack deployment. This integration offers a comprehensive framework for managing both containerized applications and virtual machine (VM) workloads within a unified system.

4.1.4 Advantages of Deploying the Kolla-Ansible Distribution

Kolla-Ansible streamlines the deployment, management, and scaling of OpenStack services, such as Zun and Kuryr, enhancing automation and reducing complexity. This method simplifies the intricacies of maintaining cloud infrastructure and promotes a uniform management strategy that enhances operational consistency across compute, storage, and networking components.

Zun [117], an OpenStack-native container management service, enables seamless operation of containerized applications, eliminating the need for external orchestration platforms like Kubernetes. Meanwhile, Kuryr serves as a bridge integrating OpenStack's networking capabilities with container environments, allowing containers to share the same network resources as virtual machines (VMs). This integration not only improves network performance but also simplifies the management of network configurations across the cloud ecosystem.

By incorporating Kuryr, containers can directly connect to OpenStack Neutron networks, leveraging Neutron's advanced networking features. This direct connectivity reduces the management overhead associated with maintaining separate networks for containers and VMs and improves overall network efficiency [118].

The combination of Zun for container management and Kuryr [119] for network efficiency creates a robust and flexible infrastructure for both containers and VMs. This setup accommodates a wide array of application deployment models, ranging from traditional VM-based applications to modern containerized microservices architectures.

Moreover, this integration reduces the operational load. Automated deployments and simplified container management through Zun, coupled with Kuryr's integrated networking, streamline daily operations such as upgrades, scaling, and network management.

The adoption of Zun and Kuryr with Kolla-Ansible not only future-proofs your cloud infrastructure against the increasing prevalence of containers alongside VMs but also enhances the agility and adaptability of your systems to new technologies and architectural patterns, thereby maximizing the return on your OpenStack investment.

In summary, each OpenStack deployment framework offers unique advantages tailored to different operational needs and preferences. Kolla-Ansible stands out for its balance of

simplicity, flexibility, and operational efficiency, making it an attractive option for numerous OpenStack deployments. Organizations are encouraged to evaluate their specific needs, existing infrastructure, and operational capabilities to select the most suitable deployment framework.

In the context of Cyber Range implementation, Kolla-Ansible an distribution of OpenStack are utilized. Kolla-Ansible leverages Docker containers, orchestrated via Ansible, to deploy OpenStack services efficiently. This approach reduces the complexity typically associated with such deployments and is particularly advantageous for those already familiar with Docker and Ansible. The configuration process, streamlined through just file `globals.yml` ensures that all aspects of the OpenStack services are appropriately managed. This method not only simplifies the installation process but also enhances the overall robustness and manageability of the OpenStack environment.

In summary, Kolla-Ansible provides a comprehensive and highly efficient solution for deploying and managing OpenStack, making it a preferred choice among DevOps practitioners for its compatibility and integration ease with Docker, and its strategic deployment across various host group affiliations optimizes resource allocation and system performance.

4.1.5 Infrastructure Environment

Two instances of ETHACA Cyber Range We implemented, both sharing the same OpenStack services and configurations. OpenStack Kolla-ansible is implemented in Ubuntu 22.04 OS and the following services are installed, Horizon, Neutron, Zun, Heat, Nova, Kuryr, Glance, Prometheus, Grafana, and Cinder. Instruction on the deployment of OpenStack with Kolla-Ansible is provided in *Appendix D*. All OpenStack services created are Docker containers The primary distinction between these implementations lies in the computer resources utilized. The OpenStack services that are deployed are presented in Figure 4.2.

The first implementation resides within the UNIWA data center, leveraging the ESXi hypervisor with the following specifications 32 GB of RAM, 2x100 GB of storage, and 16 VCPUs. The focus of this deployment is primarily centered around migrating the course

```
(cloud2) [REDACTED]:~$ openstack service list
+-----+-----+-----+
| ID | Name | Type |
+-----+-----+-----+
| 004a151144be43e89bb28bab35e913a3 | heat-cfn | cloudformation |
| 02dc90affc604f3c9dd3ff8113cd15e9 | nova_legacy | compute_legacy |
| 2b04611f6b8744c49d60aefd726bdcca | nova | compute |
| 456a902e1917417bbabd80d683f8f836 | zun | container |
| 4849818dfd894a9687500b8f2138a1d4 | heat | orchestration |
| 574c134a7dc34be6824ea4367f16e1cc | glance | image |
| 655fd533372445a2807c94788f94b6a1 | magnum | container-infra |
| 62ea9aa4b1a84b9cb85ccca7c52b2ad4 | cinderv3 | volumev3 |
| 747f04fbd7174a7c8ec722c44ce69f50 | keystone | identity |
| b83972e1f2b14b0ba4e77918feac16dd | neutron | network |
| e7a21f85585341b69cddbacc6737636 | placement | placement |
+-----+-----+-----+
```

Figure 4.2 OpenStack services

curriculum lab exercises and creating intricate scenarios within the UNIWA data center environment.

The second implementation is deployed on a local x380 laptop, utilizing VirtualBox as the type-2 hypervisor. The laptop is equipped with an Intel i5 8th Gen X380 processor, 4 CPU cores, 16 GB of RAM, and 2x 40 GB of storage. VirtualBox is configured to allocate 4 Vcores, 8 GB of RAM, 2 virtual network interfaces, and 80 GB of storage for the virtual machine hosting the OpenStack services.

Infrastructure was implemented with Heat template using Web GUI or CLI as shown in 4.3. Two main repositories Glance for local storing and hub.docker.com for Docker containers are used. To reduce resource consumption and maximize efficiency, the infrastructure environment are built-ed with Docker images using Zun API service or Magnum API service. Heat interacts with Zun container API and Kuryr network API and creates infrastructure based on containers. ETHACA Cyber Range system also supports the following container orchestration engines K8s, Swarm, and Mesos. In the future, we will include a cybersecurity scenario with COE.

The primary purpose of the ETHACA Cyber Range Platform is to facilitate cybersecurity exercises for educational, training, and research purposes. Existing exercises utilized in cybersecurity courses will be converted and ported to the platform.

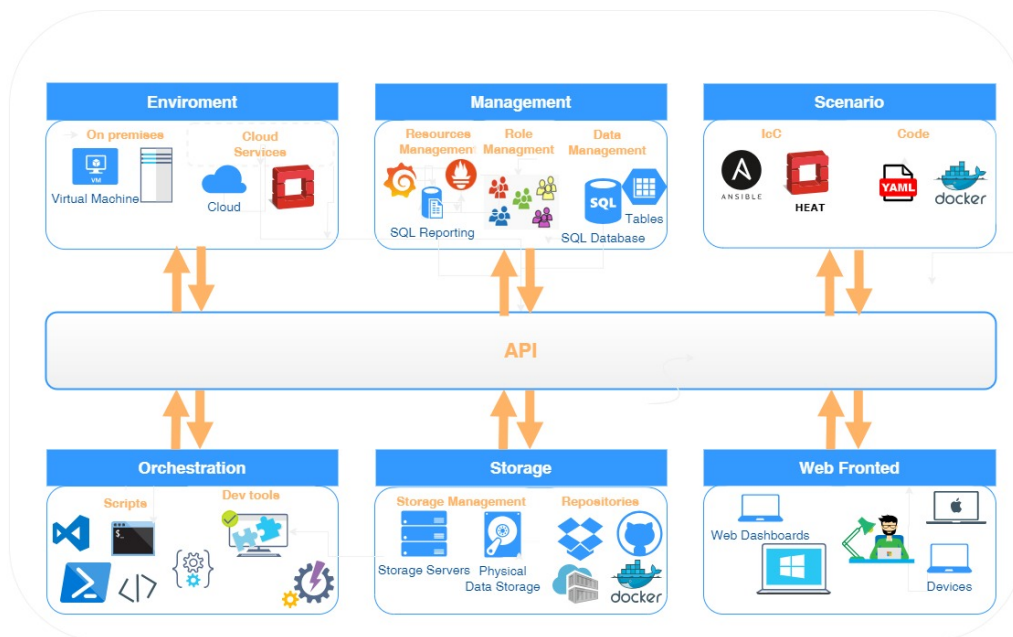


Figure 4.3 ETHACA Cyber Range.

Moreover, a key focus of the platform is to bridge the gap between theoretical knowledge and practical skills. Offering a wide array of exercises, it aims to provide students with the necessary resources to enhance their technical expertise. By applying new approaches and techniques [120], trainees will be better prepared to tackle emerging threats in the field of cybersecurity[121].

Through Infrastructure as Code (IaC) tools and automated development processes, the unified platform will streamline the workload for all stakeholders involved in creating security exercises. It will also foster collaboration between students and professors within the university, as well as encourage collaboration with other institutions. The difficulty level of the cybersecurity exercises will be tailored to the specific course type, ranging from low difficulty for undergraduate or compulsory postgraduate courses to medium or high difficulty for core or elective courses.

The exercises aim to cover a comprehensive range of cybersecurity topics offered at the University of West Attica, including system security, network security, web security, internet security, and cryptography, among others. The chance to design their exercises will be given to students, who can then include them in research-level courses or laboratory courses.

The exercises aim to cover a comprehensive range of cybersecurity topics offered at the University of West Attica, including system security, network security, web security, internet security, and cryptography, among others. Students will also have the opportunity to design their own exercises, which can be incorporated into research-level or laboratory courses.

At a research level, the following will be available to researchers and professionals:

- Development of new cybersecurity tools.
- Testing existing tools.
- Expand the platform to new sectors, such as Industrial Control Systems, OT, or IoT.
- Participate in funded European cybersecurity projects.
- Collaboration with other Universities in research and development programs.
- Conducts cybersecurity or Capture the Flag (CTF) exercises at the University, or in inter-university events, at national and international levels.

4.1.6 Learning Management System

The deployment of Moodle an open-source LMS [122] within Cyber Range systems significantly augments the educational framework for cybersecurity training. This setup provides a structured, interactive platform that is highly scalable and adaptable to the nuanced demands of cybersecurity education. The LMS [123] acts as a central component for managing course delivery, engaging users, and monitoring performance metrics effectively through its user-centric interface.

Overlaying this, the LMS offers a robust management layer that enables the organized uploading, handling, and distribution of instructional content. This content is structured into modules addressing various cybersecurity topics 4.4, such as Network Security, Malware Analysis, and Incident Response, enhanced with interactive quizzes and dynamic media content. This setup is essential for real-time monitoring and feedback, utilizing advanced analytics to track user progression and dynamically adapt learning paths based on individual

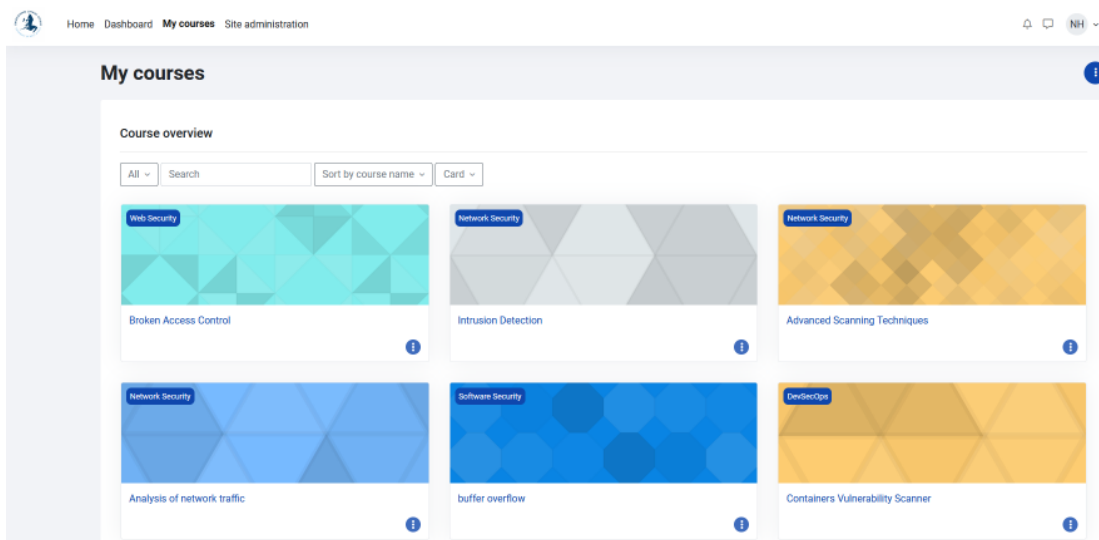


Figure 4.4 Learning Management System

performances. The infrastructure is designed to support scalable learning activities, crucial for extensive user participation.

Moreover, the LMS's forums, discussion boards, and real-time communication tools such as chat and video conferencing greatly improve collaborative learning and problem-solving capabilities. These features are vital for nurturing an interactive learning environment that promotes knowledge exchange and peer engagement.

Implementing this sophisticated system requires meticulous planning, from establishing the necessary infrastructure and configuring the LMS to synchronizing it with the cyber range's operational dynamics. The curriculum designed leverages both theoretical and practical simulations, providing an immersive experience that effectively bridges the gap between theoretical knowledge and practical application.

Ultimately, the use of an LMS within Cyber Range systems illustrates an advanced approach to cybersecurity education that blends theoretical rigor with practical engagement. This method not only improves educational outcomes but also thoroughly prepares learners for real-world cybersecurity challenges, establishing it as a critical asset in cybersecurity education and training.

4.1.7 Enhancing Monitoring and Alerting Capabilities

Prometheus stands at the forefront of the modern monitoring landscape, revolutionizing the way organizations collect, store, and analyze time-series data as illustrated in Picture 4.5. Born out of the need for a scalable and flexible monitoring solution, Prometheus has quickly gained popularity for its simplicity, reliability, and extensive feature set.

At its core, Prometheus employs a pull-based model for data collection, allowing it to efficiently gather metrics from diverse sources such as applications, services, and infrastructure components. This approach ensures minimal overhead and enables seamless integration with a wide range of systems, including cloud environments, container orchestration platforms, and microservices architectures. One of Prometheus' standout features is its powerful



Figure 4.5 Promitheus

querying language, PromQL, which enables users to perform complex analytics and derive valuable insights from their metrics data [124]. Whether it's aggregating data over time intervals, calculating rates of change, or identifying anomalous patterns, PromQL empowers users to explore their data with unparalleled flexibility and granularity.

In addition to its robust monitoring capabilities, Prometheus excels in alerting and notification management. Leveraging configurable alerting rules and integrations with popular notification services, Prometheus can automatically detect and respond to abnormal conditions within monitored systems. This proactive alerting mechanism enables organizations to

mitigate potential issues before they escalate, minimizing downtime and optimizing resource utilization.

Furthermore, Prometheus fosters a vibrant ecosystem of integrations and extensions, offering seamless interoperability with complementary tools such as Grafana, Alertmanager, and exporters for various third-party systems. This extensibility ensures that Prometheus can adapt to diverse monitoring requirements and scale alongside evolving infrastructure needs.

In conclusion, Prometheus has emerged as a cornerstone in modern monitoring architectures, empowering organizations to gain actionable insights, ensure system reliability, and proactively address operational challenges. With its robust feature set, scalability, and vibrant community support, Prometheus continues to redefine the standards for monitoring and alerting in today's dynamic environments.



Figure 4.6 Grafana

Grafana stands as a cornerstone in modern monitoring and visualization ecosystems, renowned for its user-friendly interface and powerful analytics capabilities. Within the framework of ETHACA Cyber Range, Grafana serves as an indispensable tool for monitoring and analyzing the plethora of data generated during cyber security exercises and simulations.

The integration of Grafana with ETHACA Cyber Range offers multifaceted benefits. Firstly, it provides real-time visibility into the performance and health of various components within the Cyber Range environment. System administrators can effortlessly monitor resource utilization, network traffic, and security incidents through dynamic dashboards and

customizable visualizations as depicted in figure 4.6. This proactive monitoring approach enables swift detection and response to potential cyber threats, ensuring the resilience of the Cyber Range infrastructure.

Moreover, Grafana's integration enhances the educational experience within ETHACA Cyber Range by offering insightful metrics and analytics to both instructors and students. Instructors can utilize Grafana dashboards to demonstrate cyber security concepts, showcase attack patterns, and evaluate student performance during simulated exercises. Similarly, students can leverage Grafana to gain a deeper understanding of cyber security principles, analyze attack scenarios, and refine their defensive strategies in a hands-on learning environment.

By utilizing OpenStack kolla-ansible for deployment, organizations can streamline the setup and configuration process of Grafana within the Cyber Range environment. This automated deployment approach reduces manual intervention, accelerates deployment times, and ensures consistency across multiple instances. Additionally, kolla-ansible's compatibility with OpenStack services simplifies the management of Grafana instances, allowing administrators to scale resources dynamically and adapt to evolving cybersecurity requirements.

In essence, the integration of Grafana with ETHACA Cyber Range using OpenStack kolla-ansible represents a symbiotic relationship that enhances monitoring, visualization, and educational capabilities within the Cyber Range environment. By harnessing the power of Grafana's intuitive interface and OpenStack's deployment automation tools, organizations can elevate their cyber security training initiatives and fortify their defenses against emerging threats.

4.2 Lightweight Cyber Range Functionalities and Capabilities

These technical components are interdependent, contributing to the overall functionality and effectiveness of a cyber range. By understanding and implementing these components,

organizations can create a cyber range that meets their specific training, education, and skill development needs.

These platforms provide the infrastructure backbone for cyber ranges, offering the necessary tools for virtualization, cloud services, and the management of complex, scalable environments for cybersecurity training, exercises, and research.

The next paragraphs present selected open-source lightweight Cyber Range platforms that are implemented using Docker container technology.

KYPO Cyber Range Platform (KYPO CRP)[125] is an open-source platform developed at Masaryk University in Brno. It leverages OpenStack [126] for orchestration and offers a graphical user interface (GUI) for easy access to simulated devices and networks. KYPO CRP enables the simulation of various operating systems, providing a realistic and controlled environment for cybersecurity training and research. It supports the deployment of training scenarios using Packer and Terraform and promotes reproducibility. The platform's emphasis is a graphical user interface and flexibility in device and network simulation.

Labtainers is a framework developed by Irvine et al. [127] for cybersecurity training, offering fully provisioned Linux-based lab exercises. It utilizes Docker containers within a distributed virtual machine (VM) environment, providing practical hands-on training while minimizing resource requirements. Labtainers simplify the preparation process for instructors by packaging all scenarios and configurations within the distributed VM. However, it lacks some advanced features typically found in Cyber Range platforms, such as team creation, learning analytics, and complex scoring visualizations. Overall, Labtainers offers 50 cybersecurity labs for cybersecurity training with a focus on simplicity and ease of use.

The CyExec [128],[129] deployed in with Docker containers in a VirtualBox-configured virtual environment. A practice environment are easily created for each purpose by performing vulnerability assessments and other exercise programs on assaults and defenses and running them on a Docker container. The CyExec can also be utilized collaboratively by creating an image file of a container that executes the generated exercise program and disseminating it to other organizations.

The Cyrange [42] is a Cyber Range platform built on VirtualBox VM using Docker, Docker-compose, and Vagrant. The code is available on Github. Cyrange automatically deploys and provisions virtual machines on top of Virtual Box to run scenarios involving hundreds of machines and users. Virtual machines are managed through Guacamole web interface.

Table 4.1 Comparison of Cyber Ranges Capabilities.

Cyber Ranges	Infrastructure platform	Orchestration	Isolated	Image Repository	COE
Kypo CPR	OpenStack	Terraform	Yes	Cloud-based, Linux-based, Windows-based	N/A
CyExec	Ubuntu	N/A	Partial	Docker-based	No
Cylab	Ubuntu	N/A	Partial	Docker-based	No
Labtainer	Ubuntu	N/A	Weak	Docker-based	No
ETHACA CR	OpenStack	Ansible, Heat	High	Cloud-based, Linux-based, Windows-based Docker-based images	Yes (Magnum)

In the comparison, Table 4.1 various Cyber Range platforms were assessed based on their implementation. Hence, only KYPO CPR and ETHACA CR are designed utilizing infrastructure platforms, providing the benefits of scalable and reliable infrastructure provisioning along with robust isolation capabilities that ensure secure and controlled Cyber Range environments. On the other hand, the other three platforms suffer from certain disadvantages. These platforms rely on custom-made infrastructure environments, lack proper orchestration mechanisms, and exhibit weaker isolation measures, which may compromise the security and control of the Cyber Range scenarios. Our implementation takes advantage of containerization technology managed by Ansible [130], utilizing Docker images for operating systems, applications, and systems. Among the platforms, ETHACA CR stands out due to its utilization of the Zun service. To effectively manage the containers, Zun service are employed, simplifying container management within the OpenStack environment. Zun

eliminates the need to navigate the complexities of various container technologies, enhancing accessibility and user-friendliness. This approach enhances security, integrates with the Keystone authentication service, and enables network isolation through Kuryr and Neutron integration. By designing scenarios in Docker containers, resource utilization is optimized and employ a scenarios engine that leverages Docker containers within an isolated network, offering a lightweight implementation with fully integrated authentication capabilities.

Features	Supports	Comments
Learning Management System	Yes	
Orchestration Layer	Yes	OpenStack
Underlying Infrastructure	Yes	
Virtualization Layer	Yes	Supports hypervisor-based and sw defined infrastructure.
Target Infrastructure	Yes	
Realism	Yes	
Fidelity	Yes	
Accessibility	Yes	cloud-based or on-premises (local) solution
Usability	Yes	cloud-based or on-premises (local) solution
Scalability	Yes	Supports on premise and cloud-based provisioning
Elasticity	Yes	Minimal
Curriculum	Yes	supports both ad hoc and pre-packaged curriculum

Table 4.2 Features of ETHACA Cyber Range.

According to NIST Guide [95], several essential features will help to enhance cybersecurity capacity-building. These features, which are covered by ETHACA Cyber Range as demonstrated in table 4.2, were taken into account when designing our implementation.

In summary, ETHACA Cyber Range provides several benefits, including:

- **Scalability:** ETHACA Cyber Range service provides a flexible container orchestration platform that can dynamically scale up or down based on demand. This means that Cyber Range environments can easily accommodate changes in the number of users, applications, or workloads without requiring significant manual intervention.
- **Cost-effectiveness:** A containerization is a cost-effective approach to managing Cyber Range environments. By using containers instead of virtual machines, administrators can reduce hardware and software costs, while also improving resource utilization.
- **Portability:** Containers are highly portable and can be easily moved between different environments. This means that Cyber Range environments can be easily replicated or moved to new locations as needed.
- **Resource efficiency:** Containers are lightweight and consume fewer resources than virtual machines, which means that more containers can be deployed on a given physical host. This helps improve resource utilization and reduces costs.
- **Improved security:** Containers provide a higher level of isolation between applications and users, which helps prevent security breaches. Additionally, OpenStack Zun service provides built-in security features such as encryption, authentication, and access control.
- **Automation:** OpenStack Zun service provides a powerful automation framework that can be used to automate many common tasks, such as container deployment, scaling, and management. This helps reduce the workload on Cyber Range administrators and improves operational efficiency.

Overall, the proposed Cyber Range architecture based on provides a flexible, scalable, and cost-effective platform for managing Cyber Range environments. It enables Cyber Range administrators to deploy and manage containers more efficiently and provides a higher level of security compared to traditional virtual machine-based architectures.

In the specific tests, the ETHACA Cyber Range offers a unique capability that distinguishes it from other similar range systems, such as the KYPO CRP [131]. The ETHACA

Table 4.3 Minimum requirements of OpenStack Kolla-Ansible AIO deployment for a proof-of-concept environment.

Operating System	Ubuntu 22.04 LTS
Memory	8GB
Storage	2x40gb
Network	2 network interfaces

Cyber Range excels in running test environments by utilizing orchestration for both VMs and containers. By leveraging orchestration, the ETHACA Cyber Range optimizes resource allocation and streamlines the execution of tests. It provides the flexibility to choose between VMs and containers based on the specific requirements of each scenario. This adaptability allows for efficient resource utilization, resulting in reduced computation resources and execution time compared to similar Cyber Range systems.

Compared to CyExec, the ETHACA Cyber Range provides several advantages. Firstly, the ETHACA Cyber Range can run and manage the scenario environment infrastructure using structured orchestration templates, ensuring a streamlined and consistent setup across multiple scenarios. Secondly, the ETHACA Cyber Range offers enhanced flexibility by providing users with the choice to run scenarios either as containers or virtual machines (VMs). This flexibility empowers users to select the technology that best aligns with their specific requirements. Moreover, the ETHACA Cyber Range seamlessly integrates with the authentication service, ensuring secure access and user management within the range environment. This integration enhances the overall security posture and facilitates proper user authentication and authorization. Furthermore, the ETHACA Cyber Range enables network isolation, allowing for the creation of isolated network environments for individual scenarios. This ensures that each scenario operates in its own isolated network space, preventing interference and providing a more realistic and controlled testing environment.

Chapter 5

Enhancing Cybersecurity Competence through Cyber Range

Despite the abundance of cybersecurity courses available, the EU faces a shortage of cybersecurity skills in the European labor market, and it has to improve the substance of the courses offered to students [132]. Data breaches and cyber-attacks targeting critical infrastructures are examples of the more frequent and sophisticated cyber-attacks. To tackle these challenges and their constant evolution, there aren't enough cybersecurity professionals with the necessary expertise. Businesses and government agencies are all severely impacted by the global scarcity of experienced cybersecurity professionals. According to estimations, almost half a million jobs must be filled, and the workforce must grow at least sixty percent to fulfill the expectations of US businesses [133].

Companies are vulnerable to various cybersecurity threats due to their failure to attract and retain experienced cybersecurity experts. Insider attacks further increase companies' problems and make it very difficult to deal with, mitigate or detect them [134]. According to Gartner, by 2025, over half of major cyber incidents will be attributed to a shortage of skilled professionals [135].

Interest in Cyber Ranges has been steadily growing as their applications across various domains become more pronounced. These systems are primarily used for three main objectives: research, training, and exercises.

- This involves testing and validating implementations such as methods, tools, and complete systems within a controlled and isolated environment that is nevertheless complex enough to facilitate the development and testing of new tools or the design of novel attack techniques and methods.
- Cyber Ranges play a critical role in academia and professional development, including specialized security courses and cybersecurity certifications. They provide a practical, hands-on context where theoretical knowledge is applied in simulated real-world scenarios.
- This category includes the use of Cyber Ranges for cybersecurity training exercises such as Capture the Flag (CTF), Cyber Defense Exercises, and other competitive formats like Table Top Exercises and attack/defense simulations. These exercises are not only popular but also integral in honing the skills of participants in realistic, competitive settings.

5.1 Innovative Cybersecurity Training through Cyber Ranges

Preserving educational programs up to date with the constantly changing nature of cyber threats, providing students with meaningful experiences—particularly through practical application—and ensuring that the material is relevant and appropriate for all technical skill levels are the main challenges to increasing the effectiveness of cybersecurity training [136]. Another major issue is determining how effective training programs are in improving cybersecurity policies and behaviors inside businesses. To overcome these challenges, innovative approaches to training design are required. These include the use of gamification, digital twins, and adaptive learning technologies, as well as a commitment to ongoing development and alignment with current cybersecurity trends and threats.

Cyber ranges provide educators with a useful, interesting, and efficient tool for cybersecurity education, according to Beauchamp et al. [137]. Such environments offer students first-hand exposure to real-world situations, improving their technical expertise and pre-

paredness for the workforce. Cyber ranges keep students engaged and motivated in their education by simulating real issues regarding cybersecurity. Additionally, they provide potential learning experiences that meet the needs of students at all skill levels, from novices to experts. Moreover, cyber ranges prepare students for employment in cybersecurity by bridging the knowledge gap between theory and practical practice.

5.1.1 Behavioral strategies

In the current realm of cybersecurity, the role of humans is still crucial in protecting data from ever-changing threats. Although technology improvements contribute to strengthening defensive capabilities, the final efficiency of security measures depends on the behaviors and actions taken by personnel within businesses. Consequently, there is an increasing acknowledgment of the significance of behavioral methods in improving the effectiveness of cybersecurity training. Behavioral strategies involve an extensive number of tactics that are designed to influence human behavior to achieve desired security objectives. These tactics frequently utilize principles from behavioral psychology and organizational behavior to promote security-conscious attitudes and decision-making among individuals. Behavioral techniques can successfully enhance technical controls in lowering cybersecurity risks by targeting cognitive biases and social factors that influence behavior. For instance, Herath et al. [138] devised a framework rooted in protection motivation theory to bolster adherence to security policies by manipulating individuals' perception of the severity of the threat, their vulnerability to it, and their self-efficacy. These research efforts emphasize the capacity of behavioral tactics to impact human behavior and enhance defenses against cybersecurity threats.

To successfully employ behavioral tactics in cybersecurity education, it is important to incorporate the most effective methods based on empirical research and industry expertise. Effective strategies involve customizing training materials to align with the specific preferences, knowledge levels, and learning styles of individual learners to enhance their engagement and motivation. Providing incentives and rewards for behaviors that prioritize security helps to strengthen desired activities and promote continued adherence. By using

social norms and leveraging peer pressure and social comparison, it is possible to encourage people to follow security policies and establish a culture where everyone feels responsible for security. Regularly evaluating the success of training using measures such as knowledge retention, behavior change, and security incident rates enables ongoing development and enhancement of training interventions. Cybersecurity training programs can strengthen organizational resilience against cyber threats by using evidence-based behavioral methods, utilizing theoretical models, and following best practices. These programs effectively engage trainees, promote security awareness, and encourage behavioral change.

The acknowledgment of human aspects in cybersecurity has led to a shift in thinking towards a security approach that places greater emphasis on human needs and behavior. Gerber et al. [139] claim that although technical solutions are crucial, they must be augmented by endeavors to comprehensively comprehend and successfully shape human behavior. Individuals must actively engage and cooperate to effectively counter sophisticated cyber attacks, as technical safeguards alone may not be enough. Therefore, cybersecurity training programs must give priority to initiatives that focus on changing behavior. This will help in developing a culture that is conscious of security and allow employees to actively protect against cyber threats. Gamified learning is an effective method for cybersecurity training that uses game design ideas to inspire and involve learners. Gamified platforms promote active engagement and information retention among trainees by incorporating features such as competition, awards, and advancement [140]. Xiao et al. [141] conducted a systematic literature review that emphasized the beneficial effects of gamification on cybersecurity education. These effects include heightened motivation, enhanced information acquisition, and behavioral changes. Moreover, gamified simulations provide learners with the opportunity to hone their cybersecurity capabilities in a secure and regulated setting, hence enhancing the integration of acquired knowledge into real-life situations.

Digital twins provide a new method for analyzing behavior in cybersecurity education programs. Digital twins allow trainers to watch and analyze human behavior in response to simulated cyber threats by constructing digital clones of persons or organizational processes [142]. This recurrent interaction enables the implementation of focused treatments and

individualized coaching to target behavioral weaknesses and strengthen desired security habits. Moreover, digital twins enable the examination of intricate cyber situations and the evaluation of trainees' ability to make decisions in a safe environment, thereby improving the efficiency of cybersecurity training programs.

To optimize the effectiveness of cybersecurity training, businesses should implement a comprehensive approach that incorporates behavioral methods into their training frameworks. Von Solms [143] supports the implementation of comprehensive training programs that accommodate various learning styles and preferences. Organizations may cultivate a culture of security awareness and compliance by utilizing gamified learning, digital twins, simulations, and other interactive methods to create immersive learning experiences. Furthermore, continuous evaluation and reinforcement mechanisms are crucial for preserving changes in behavior and maintaining the lasting efficacy of cybersecurity training activities.

5.1.2 Insider Threat

Cybersecurity must account for human factors and integrate these insights into the design of systems and security policies. By considering the behavioral aspects of cybersecurity, organizations can better understand and mitigate insider threats. This approach aligns with the interdisciplinary framework that combines insights from IT, criminology, psychology, and human factors to create a holistic security strategy. This comprehensive approach not only addresses the technological aspects of cybersecurity but also considers the human elements, ultimately leading to a more secure organizational environment.

Mitigating insider threats requires a comprehensive approach that combines technological solutions with a deep understanding of human behavior. Given that insider threats are often facilitated by individuals who have legitimate access to an organization's systems, traditional cybersecurity measures like firewalls and intrusion detection systems may not be sufficient. Effective mitigation strategies should include rigorous access control measures, continuous monitoring, and the implementation of strict data usage policies.

One critical aspect of mitigating insider threats is the incorporation of behavioral cybersecurity [144]. This involves understanding the psychological and social dynamics that

might lead an insider to act maliciously. Regular training and awareness programs can help educate employees about the potential risks and encourage a security-conscious culture within the organization. Additionally, implementing user behavior analytics (UBA) can help in detecting unusual activities that might indicate an insider threat. By analyzing patterns and anomalies in user behavior, security teams can identify potential threats early and take preventive action.

Insider threats in cybersecurity refer to risks posed by individuals within an organization who have access rights and operate behind firewalls, making their actions particularly dangerous and challenging to detect. This issue is widely acknowledged as critical for cybersecurity management. Surveys, such as the SANS Healthcare Cyber Security Survey, have highlighted that careless insiders are often perceived as significant threats due to human behavior factors. To address insider threats effectively, understanding the behavioral aspects of cybersecurity is crucial. Behavioral cybersecurity involves studying the profiles and methods of hackers, including insiders, and applying psychological and social theories to understand their motives. This approach can help in predicting and mitigating potential security breaches by considering human factors in system design and security policies. Integrating behavioral insights into cybersecurity can lead to more robust and comprehensive security programs.

Two categories of insider threat mitigation can be identified a) technical mitigation approaches, like the IDS, SIEM, DLP, ACS, and honey-tokens, and b) non-technical mitigation approaches, like the psychological prediction, security education and awareness, information security policy, and the hybrid insider threat prediction model. This categorization is fundamental for an organization as a way to moderate these insider threat issues. [145].

5.1.3 Technical Controls to Identify Insider Threats

To identify and isolate an insider, any related activity should be recognized as suspicious or malicious. Approaches that address this problem only from a technical point of view, cannot include the substantial part of human behavior [134]. The most appropriate technical controls combine malicious activity monitoring with the insider's behavioral characteristics. Two main categories can be identified. The first consists of event monitoring and applies

methods to distinguish unauthorized activities from authorized ones, and the second focuses on the user's behavior and attempts to recognize an insider's intent for a malicious activity or an attack. To cover all types of activities, technical control tools could be implemented on networks, hosts, and the cloud.

Intrusion Detection Systems (IDS)

Intrusion Detection Systems serve as a second line of defense to enhance the security mechanisms applied to a system and cover the prevention part of its security framework. Using a variety of detection engines, they aim to make a distinction between events that violate the security of a system and those that do not. The captured information necessary for the detection process is normally huge, and, therefore, further processing is required to reduce its amount [146].

An effective IDS should be designed and implemented to also detect insiders by locating behavioral deviations from normal activity, that may lead to data breaches or losses. However, an IDS has serious limitations in dealing with insider threats, such as a high number of false alarms, a huge database log file size, and the requirement that an administrator must analyze the traffic and the user's behavior continuously. Among its drawbacks is also the lack of encrypted traffic monitoring. Consequently, IDS are not the ideal candidate for detecting insiders, but the. IDS's main focus is the external attackers.

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a special tool that analyzes and gathers together, in one management platform, information derived from logs. SIEM collects information through secure network channels, and, among others, a variety of security-related logs, workstation logs, and application logs (e.g. client workstations, servers, antivirus systems, network devices, honeypots, firewalls, IDS). After collection, SIEM correlates all this information [147]. Based on this final correlated data, a security administrator can attempt to identify possible insider activity before it harms the system. After an incident, he may conduct forensic analysis.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is a technology responsible for the early detection of data exfiltration attempts by an insider. It is performed in three steps: a) System discovery: scanning storage devices, capturing network data flow, and watching user behavior on endpoint devices. b) Leaked confidential data identification: information discovered in the system discovery step could be identified if it is secret information using techniques like keyword matching, regular expressions, or hashing fingerprinting. c) Organization policy enforcement: this step prevents any action that could cause any security breach in the identified confidential data in the previous step [148].

The benefit of using a data loss prevention approach is that we can use it to protect three types, or parts, of data in an organization, depending on the business needs. These types are (i) data at rest (ii) data in motion (iii) data in use.

Access Control System

Access control is a suite of mechanisms that aims at protecting the resources of a system from unauthorized access. It includes the assignment to subjects (authentication) of permissions to objects (authorization). There are several types of rules based on principles, like allocation of least privileges, privilege escalation, or isolation. All these in general have the purpose of prohibiting unauthorized access to system resources and enforcing authorized access appropriately. But what happens when the subject is an insider? Regardless of the model applied, Role-Based Access Control (RBAC), Mandatory Access Control (MAC), or Discretionary Access Control (DAC), an insider is a special type of user that uses access controls in a system. He can easily bypass them, misuse them, and then behave maliciously for his purposes and interests.

Honey-tokens

A honey token is a method used to attract malicious insiders and helps to detect, identify, and confirm a malicious insider threat [149]. Moreover, it may be effective in catching insiders

who are snooping around a network. The honey token is a technique that is part of the honeypot technology [90]. However, it is different from the other types because it could be any interactive digital entity, such as a Microsoft Office document, rather than a hardware device or software. The main concept is that no one should interact with the trap, and any interaction with the digital entity will indicate to the security administrator that there could be a threat of a malicious insider.

As an example, if a company's General Management (GM) suspects that one of their IT staff is checking their emails because an IT employee has full authorization to access emails, then they could use the honey-token approach to generate an email to the GM. This email should contain interesting information to attract an insider. Then, this honey token leads the insider to use a username and password within the email to access the honey token, as no one else has this username and password. When a malicious insider accesses the URL, insider information such as the IP address, device name, and user domain name will be sent to the IT security team to deal with this breach.

5.1.4 Non-Technical Approaches

It has been seen that insiders manage to avoid technical controls at least on the prediction phase. This constitutes proof that insider threats should also be faced from different points of view, such as through prediction, training, awareness, and appropriate security policies.

Psychology Prediction

Stemming from the psychological state and the behavior of the operators, observers have identified certain psychological indicators associated with a malignant inside menace. These contributors are motive, opportunity, and capability.

Security Education and Awareness

Internal menace mishaps could be prevented using specialized training on security awareness, laying due emphasis on the aspect of the internal menace that is not pre-meditated. According

to the Ponemon Institute [150], more than 62% of organizations carry out training sessions regularly for advanced operators in the context of shielding the organization against inside threats, thus allotting 11% of their IT financial resources to security training and awareness. This type of training may also incorporate guest speakers, classroom seminars, workshops via the Internet, updated feedback inflow from the organization's internal Internet site, e-mail addresses and social media, and even printed handouts. The training itself could range from standard incident reporting and accountability guidelines to impact and penalty measures, from processing sensitive data to copyright protection, as well as internal threat red flags, psychological manipulation fraud to extract valuable information (social engineering), and last but not least, unintended outflow of information.

Information Security Policy

The organization's data protection strategies impose a set of guidelines that constitute the control mechanism regulating the organization itself once it has fully identified its targets. These strategies are presented in a statement where the operators explicitly express their expectations concerning an organization, and what they are anticipated to perform about data security, including the appropriate behavior and the acceptable work ethics within the organization [87]. Nevertheless, very often the operators do not comply with the security strategy mainly due to two main reasons. Either the strategy is underdeveloped or the operators are not fully informed of the security strategy.

Consequently, if the data protection strategy is not unanimously exercised by all the authorized operators, then the risk factor of unintended internal threat rises dramatically. In September 2014, the USA Department of Defense issued a specific set of regulations given both setting and securing an effective nationwide policy against inside threats within the Department of Defense [151]. This policy averts, discourages, identifies, and alleviates actions by malignant insiders who pose a threat to the country's national security or to the Department of Defence staff, amenities, operations, and resources.

Hybrid Insider Threat Prediction Model

The above-discussed technical and non-technical mitigation measures can also be combined into a hybrid approach. Such insider threat prediction models, as proposed in [152], firstly analyze misbehavior in data systems at the actual time of occurrence based on data accumulated from Honeypots, Intrusion Detection Systems, and system calls. Then, psychological profiling issues like the anxiety level, the system purpose, and the operator's elaborateness and dexterity are inserted into the analysis.

5.1.5 Gamification

Recently, there has been a rise in the literature on the advantages of incorporating game design and features into non-gaming domains, such as education, with predominantly favorable outcomes [153]. The primary goal of gamification is to enhance involvement and connection with educational material, stimulate learners' motivation, and enhance learning results. Studies indicate that gamification not only has a positive impact on the intervention itself but also enhances overall attitudes towards a specific subject and enables users to effectively use the acquired skill in their surroundings [154]. The use of gamification is especially valuable in areas like cybersecurity, where the information is frequently technical, sophisticated, and subject to constant changes as hackers modify their technology, methods, and techniques. The ability of gamification to motivate users to consistently engage with challenging knowledge is what makes it particularly ideal for cybersecurity.

While people are considered superior, there are certain jobs that they are required to perform that are difficult to easily generate interest or pleasure, and hence, do not create intrinsic drive. This encompasses cybersecurity awareness, training, and education initiatives that numerous companies require their staff to participate in, to decrease the risk of a cyber attack.

The concept of self-determination theory, as discussed by Ryan [155], examines the process of transforming external motivation into a more internally regulated form in the absence of intrinsic motivation. In general, extrinsic motivation can be classified into two

categories: external motivation, which involves the use of rewards or punishments, and internal motivation, which involves educating employees about the actual value of the behavior. Although rewards can be effective in influencing behavior, it is the incorporation of the real importance of an action that is more likely to lead an employee to self-sufficiently choose to participate in training, even if they are not interested in the subject [156]. The self-determination theory suggests that three important factors promote fact self-motivation: competence, autonomy, and relatedness [155]. The above factors indicate that for employees to actively participate in training, they need to believe that it will help them achieve personal development, have the autonomy to set their own goals related to this development, and perceive that the intervention will facilitate interactions with others [157]. Hence, every cybersecurity awareness, training, and education initiative must aim to equip staff with the necessary capabilities to directly address these components. Gamification and serious games have been identified to enhance motivation and boost competence by offering an enjoyable and captivating learning experience that specifically focuses on self-determined incentives.

Games are typically characterized as planned activities that individuals engage in for enjoyment, such as sporting events like basketball or board games like Chess. The industry of digital gaming is a highly productive market, with approximately 40% of the global population being online gamers and 88% of young adults being deeply involved in the digital gaming realm [158]. Games are now being used for purposes beyond entertainment. Their concept and principles are being adapted to non-gaming situations to provide enjoyable learning experiences, as demonstrated by Hew and Du (2024). Some examples of educational tools in the field of cybersecurity are CyberCEIGE, a training that takes place in a 3D virtual world, and Control - Alt - Hack, a challenging board game that is aimed at both students and security experts [159].

Serious games refer to the adoption of game design principles in educational settings to enhance players' proficiency in specific areas, such as cybersecurity training. This includes including instructional instructions, investigation, strategy development, and simulating responses [160]. The utilization of a gamified framework attempts to support users in unifying many aspects of cybersecurity behaviors inside a single environment, enabling them

to attain expertise through experiments, typically at an accelerated rate [161], [162]. Serious games can enhance self-determined motivation by offering an enjoyable experience that can boost feelings of competence and autonomy. For instance, individuals can freely practice skills like identifying phishing emails in controlled settings until the desired behaviors become automatic. Augmented reality has been discovered to enhance the advantages of serious games as an intervention by fully engaging players in the learning experience through the integration of actual and computer-generated environments [161]. It is crucial to acknowledge that these enhancements may incur expenses for businesses, potentially posing challenges for small to medium-sized enterprises to implement.

Gamification is a concept that involves applying game principles to the design of a serious game to enhance participation, efficiency, and incentive to interact [163], [164]. Gamification has been shown to improve cybersecurity awareness interventions by promoting decision-making through feedback that improves perceived competence, offering various options to increase self-determination, and providing an online community for shared learning and competition [165]. For instance, the user's belief in their ability to generate passwords can be enhanced by incorporating progress bars to promote self-assessment and leaderboards to foster comparison with others' abilities [163]. By offering employees a platform for hands-on cybersecurity exercises through gamified learning, participants will be motivated to actively participate in content that enhances their motivation and skill development, leading to successful behavior change.

Recently, several educational initiatives in the area of cybersecurity focused on raising awareness through seminars or lectures. These events aimed to provide information to a large audience without providing customized training for certain audiences. These initiatives prioritized the dissemination of a large amount of information within a limited timeframe but were unsuccessful in effectively conveying particular expertise. Although training may have resulted in an initial improvement in comprehension, research has shown that it does not accurately represent the audience's ongoing expertise [166]. The problem was accurately recognized as being related to the method of delivering the cyber awareness education, rather than the material itself citecrookall2010serious.

Cybersecurity exercises have emerged as highly effective and efficient means of imparting key skills and experience in the field of cybersecurity, particularly when replicating elevated cyberattack incidents. The scenarios can be customized for specialized sectors such as electricity, transportation, or health care. They can address technical aspects or business aspects. Cyber Range Exercises (CRXs) have become essential in bridging the cybersecurity workforce gap for enterprises, as stated by Glas et al. (2023), Chouliaras et al. (2021), and Gomez et al. (2023) in their respective studies [167, 94, 168]. Their research highlights the effectiveness of CRXs in improving professionals' capabilities to address emerging cyber risks, hence enhancing overall organizational resilience and security protocols. Cyber ranges are used to conduct organized exercises that enable firms to effectively educate their workers in responding to cybersecurity incidents that pose a threat to their assets or their whole organization.

The knowledge and expertise of individual users who engage with or operate an organization or system are among its most critical resources. These personnel may include system administrators, staff members who regularly engage with or have a certain level of authority over many apps, or external users or partners. Several recent reports highlight the shortage of well-educated cybersecurity professionals who are essential for protecting these systems. Aside from the limited number of experts in the field, there is a significant lack of crucial cybersecurity skills among users that are directly relevant to their specific duties [169]. Europe has created the European cybersecurity skills framework to address these needs. This framework serves as a practical tool for identifying the specific skills required for each cybersecurity function [170].

5.1.6 Utilization of the European Cybersecurity Skills Framework

In addition to the widespread adoption of guidelines such as the NIST Cybersecurity Framework, the European Cybersecurity Skills Framework (ECSF) [171] has emerged as a critical tool under the auspices of the European Union Agency for Cybersecurity (ENISA). Both frameworks play a pivotal role in the development of the ETHACA Cyber Range, providing a comprehensive set of standards that guide the simulation environments and training modules

offered. This integration ensures that the Cyber Range not only adheres to international cybersecurity practices but also aligns with European-specific requirements, thereby fostering a versatile and robust educational setup.

The Ethaca Cyber Range uniquely synthesizes the strategic insights from the NIST framework with the detailed role-based competencies outlined in the ECSF. By doing so, it offers a training platform that is both globally relevant and tailored to the European context. The NIST framework's focus on identifying, protecting, detecting, responding, and recovering from cyber incidents complements the ECSF's role-specific skill sets, thereby enhancing the realism and educational value of simulations. This dual-framework approach equips students with the skills necessary to navigate and mitigate diverse cybersecurity challenges effectively, preparing them for roles that require adherence to both EU regulations and global cybersecurity standards.

The ECSF serves to standardize and clarify the requisite skills and competencies needed across the cybersecurity profession, ensuring a comprehensive, harmonized approach across the EU. By defining specific roles and the skills they require, the ECSF facilitates targeted educational initiatives, allowing training programs to address the precise needs of the cybersecurity industry effectively.

At the University of West Attica (Uniwa), the Cyber Range offers a state-of-the-art simulation environment designed to provide practical, hands-on experience to those engaged in cybersecurity education and training. This facility is pivotal in implementing the ECSF by providing an immersive learning experience where theoretical knowledge is applied to real-world cyber threat scenarios. Specific roles outlined in the ECSF such as Cyber Incident Responder, Cyber Threat Intelligence Specialist, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Digital Forensics Investigator, and Penetration Tester are particularly suited to benefit from this type of experiential learning. For each role, the Cyber Range can simulate specific scenarios that reflect the competencies and tasks described in the ECSF.

Cyber Incident Responders practice identifying and mitigating attacks in a controlled, but dynamic environment mirroring actual threat landscapes.

Cyber Threat Intelligence Specialists engage in activities such as data collection and analysis, simulating the production of actionable intelligence reports.

Cybersecurity Educators use the range to demonstrate live cybersecurity challenges and defenses, enhancing their teaching with real-time demonstrations.

Cybersecurity Implementers and Researchers test and refine security solutions and innovative concepts against emerging cyber threats.

Digital Forensics Investigators explore forensic data extraction and analysis techniques on systems compromised in a controlled manner.

Penetration Testers conduct controlled attacks on systems to identify vulnerabilities and test the effectiveness of existing security measures.

This practical application of the ECSF via the Ethaca Cyber Range not only reinforces the theoretical components of cybersecurity training but also enhances the skill sets of participants, making them industry-ready upon completion of their courses. The Cyber Range's ability to adapt to different roles and scenarios as specified by the ECSF allows to address the skills gap in the cybersecurity workforce, ensuring that graduates are not only familiar with European standards but are also capable of executing their roles with competence and confidence in diverse and challenging environments.

5.2 Cyber Security Exercises

Training enhances participants' levels of awareness, knowledge, and preparedness. Organizations, companies, universities, and government agencies create cybersecurity incident response teams (CSIRTs) and Information Sharing and Analysis Centers (ISACs) for knowledge sharing and cooperation between public and private sectors [172].

Cybersecurity exercises improve capacity building which makes participants better equipped to handle security situations [173]. Exercises help participants to develop both technical and non-technical skills, particularly soft skills that are crucial but usually missing from cybersecurity professionals, probably because some environments are not simply tactile [174]. Cybersecurity exercises are planned to identify vulnerabilities in systems,

mind the gaps in procedures, and train the security incident response teams (CSIRTs) in real-situation scenarios. Usually is conducted [175] or every two years at national and international levels[176],[2] to fulfill various purposes such as educational, military, and capability enhancement on different platforms with different objects.

There are three main categories of Cybersecurity exercises: Cyber Defense eXercises (CDX), Table Top Exercises (TTX), and Capture the Flag (CTF) [177].

CDX has been acknowledged as a successful method for conducting cybersecurity awareness training but is also the best tool for determining and categorizing the various security requirements of every industry. Students are given the best opportunity to enhance their knowledge of insuring and defending information systems, and their progress is evaluated in the context of real-world situations [68]. TTX [178, 179] are designed to enhance and refine practical skills through hands-on experiences. These activities foster teamwork, communication, and problem-solving capabilities while also enhancing understanding of corporate protocols. By developing these competencies, professionals will be better equipped to contribute effectively to cybersecurity teams. A Capture the Flag (CTF) is a practical exercise designed to enhance cybersecurity skills [180] and provide valuable learning opportunities through different formats, such as jeopardy, attack-defense, and a combination of the two. However, participating in CTFs does not assure future success since contestants often receive limited feedback on their performance, which is essential for effective learning[181].

5.2.1 Design and Use of Cybersecurity Exercise Templates

The essential steps required to design and develop a cyber security exercise encompasses defining objectives, selecting an approach, crafting network topology, devising a scenario, setting rules, choosing appropriate metrics, and compiling lessons learned [182], [183]. Recognizing the strategic importance of proactive preparedness and resilience-building exercises, we propose a comprehensive Cybersecurity Exercise Template as shown in Appendix F.

This template is designed to serve as a blueprint to simulate real-world cyber attacks in a controlled environment, enabling them to assess, refine, and enhance their response strategies. The core objective is not only to test the technical defenses but also to bolster the human

elements of cybersecurity—awareness, reaction time, decision-making under pressure, and interdepartmental communication.

The proposed template outlines a structured approach to crafting realistic, scenario-based exercises tailored to the specific threats and vulnerabilities relevant to the university. By integrating detailed components such as the Objective, Target Audience, Scenario Overview, Threat Actor Profile, and Attack Vector and Methodology, the template ensures a comprehensive coverage of essential aspects of cybersecurity preparedness.

Furthermore, the template emphasizes the importance of post-exercise analysis through its Evaluation Criteria and Feedback and Improvement Plan sections. This not only facilitates a continuous learning process but also fosters a culture of continuous improvement in cybersecurity practices.

5.3 Conclusions

This chapter examined numerous techniques, including gamification, and behavioral tactics, to improve the effectiveness of cybersecurity training. Our research indicates that implementing these strategies might greatly enhance the level of cybersecurity within organizations as well as the effectiveness of cybersecurity education and training. Our study suggests that cybersecurity risks can be greatly diminished when training programs are crafted to tackle cognitive biases and the impact of social influences on behavior [136].

Gamification has become an effective method for improving the acquisition of cybersecurity expertise while engaging students. Integrating designing game aspects within educational contexts enhances participation, incentive, and the practical application of learning. Our analysis reveals that gamified learning environments, characterized by their constantly evolving and competitive nature, can significantly improve students' engagement and memory of intricate cybersecurity concepts. Cyber ranges are an important factor in bridging the knowledge disparity between theoretical and practical aspects of cybersecurity training.

To summarize, the combination of gamified learning, Cyber Ranges, and behavioral strategies in cybersecurity education and training initiatives offers a holistic approach to

educating individuals about the intricacies of the digital age. This study advances this topic by highlighting how these state-of-the-art techniques may enhance cybersecurity abilities and foster proactive, security-conscious societies. Training programs need to be modified to present professionals with the necessary information and skills to defend against constantly changing threats in an era of progressively advanced cyberattacks.

We highly recommend conducting additional research to explore the long-term impact of these tactics on the cybersecurity resilience of companies. It is crucial to investigate novel approaches for enhancing cybersecurity training, to discover revolutionary strategies that greatly enhance resilience against cyber threats.

Chapter 6

Use Case Scenarios

Critical National Infrastructures are the main targets of cyber attacks since essential information or services depend on their systems and their protection becomes a significant issue that concerns both organizations and nations [6–9]. Attacks on such critical systems include penetrations to their network and installation of malicious tools or programs that can reveal sensitive data or alter the behavior of specific physical equipment [10]. The majority of chief information security officers around the world are worried about the cybersecurity skills gap, with 58% of CISOs believing the problem of not having an expert cyber staff will worsen [184].

Our goal is to design complex scenarios that support a set of characteristics of Cyber Range platforms, such as automated deployment, high availability, scalability, reusable resources, and isolation. For the deployment, OpenStack delivers a Heat orchestration module to increase the scalability and performance of scenarios. Using configurable YAML templates, Heat orchestration is responsible for controlling the provision of services, applications, and infrastructure. Instead of creating different operations such as instances, volumes, security groups, floating IPs, and images individually, we can define a STACK that consists of a set of resources in a text file written in YAML format.

This section presents diverse use cases of the proposed Cyber Range system, examining its effectiveness across various scenarios. By exploring practical applications, it aims to provide a comprehensive assessment of how the Cyber Range can be utilized in real-world

settings. Each use case is meticulously described and evaluated to demonstrate the system's capabilities and limitations.

The analysis includes scenarios such as WordPress injection attacks, SQL injection vulnerabilities, detection of malicious network traffic, and advanced scanning techniques. These use cases represent common challenges faced in cybersecurity, offering insights into the system's practical applications and its potential to enhance cybersecurity training and research.

6.1 WordPress injection

A company has deployed a WordPress website on a cloud infrastructure platform using a Heat template for provisioning the required resources such as virtual machines, storage, and networking components. The website is built on WordPress version 5.0, which is known to have multiple security vulnerabilities. An attacker scans the website using WPScan, a popular open-source tool that can scan WordPress websites for vulnerabilities. He discovers a critical vulnerability, CVE-2020-28036, which allows attackers to gain privileges by using XML-RPC. The attacker attempts then to exploit the vulnerability by commenting on a post using XML-RPC and successfully gains elevated privileges. With elevated privileges, he can access sensitive data, install malicious plugins or themes, and potentially take control of the website. The attacker uses Metasploit, to gain full access to the website and execute arbitrary code. The attack is successful because the website was not updated to the latest version of WordPress, and the Heat template in the scenario did not include all the appropriate security measures such as WAF, IDS, or monitoring tools to prevent and detect attacks.

The infrastructure provision was developed with the OpenStack Heat Template (HOT) written in YAML language. The attacker's host, the database, and the web server are Docker images. WordPress is a specific version preconfigured Docker image file with CVE-2020-28036 vulnerability [185]. Heat stack template written in YAML infrastructure code is illustrated in Figure 6.1.

The scenario can easily be modified and reused by adding a different network topology to the infrastructure or changing the version of WordPress injecting vulnerable code only with a few lines of code. Docker images are stored in the local repository and can be uploaded to [hub.Docker.com](https://hub.docker.com).

```

outputs:
  url:Vulnerable Site url
  value:
    {get_attr: [floating_ip, floating_ip_address]}

resources:
  association:
    properties:
      floatingip_id: { get_resource: floating_ip }
      port_id:
        {get_attr: [wordpress, addresses, private-network, 0, port]}
    type: OS::Neutron::FloatingIPAssociation

  wordpress:
    type: OS::Zun::Container
    properties:
      image: "wordpress:5.0"
      environment:
        WORDPRESS_DB_HOST:
          {get_attr: [db, addresses,private-network, 0, addr]}
        WORDPRESS_DB_USER: root
        WORDPRESS_DB_PASSWORD: rootpass

  db:
    type: OS::Zun::Container
    properties:
      image: mysql

```

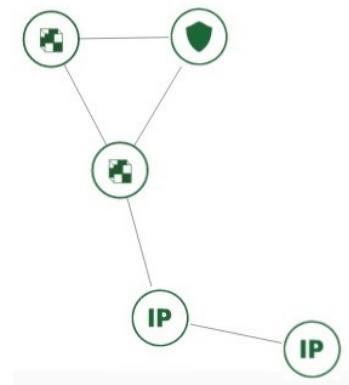


Figure 6.1 Part of Heat Template Code at WordPress Vulnerable Scenario and Stack Topology deployed via the Horizon Dashboard.

6.2 SQL injection vulnerability

In the second scenario (Figure 6.2), we use the vulnerable website, Damn Vulnerable Web Application (DVWA), to learn the SQL injection vulnerability. The tool we will use to find the vulnerability is SQL Ninja. The scenario's primary educational objective was to obtain participants on how to identify an SQL injection on a website.

In the following scenario, a trainee wants to learn how to identify SQL injection vulnerabilities on a website. A testing environment is set up using Docker containers. One container contains the vulnerable website DVWA, which is a deliberately insecure web application that contains several vulnerabilities, including SQL injection. Trainee launches another Docker container containing the SQL Ninja tool, to access the DVWA website [186],

and uses SQL Ninja to scan the DVWA website for SQL injection vulnerabilities. The tool automatically identifies the vulnerable input fields and suggests SQL injection payloads to test the vulnerability. In the next step, the attacker selects a suggested payload and executes the SQL injection attack. SQL Ninja identifies the SQL injection vulnerability and displays the results, including the type of vulnerability, the SQL query that was executed, and the results of the query. Finally, it analyzes the results and understands how the SQL injection vulnerability can be exploited to gain unauthorized access to the database. We can repeat the process with different payloads and input fields to gain a better understanding of how SQL injection attacks work.

In particular, infrastructure at SQL injection scenario was created in an Ansible YAML file. As a result, using the knowledge gained from this scenario, we can identify SQL injection vulnerabilities on other websites and provide recommendations for fixing them. Hence, the trainees are capable of comprehending the basic ideas of web security by establishing the vulnerable site and technically examining the vulnerabilities during the SQL injection by following and executing the cybersecurity scenario.

```
- name: SQL Injection Scenario
  hosts: localhost
  gather_facts: false
  tasks:
  - name: Deploy an instance
    os_server:
      state: present
      name: sqlninja
      image: Ubuntu
      key_name: sql_key
      timeout: 200
      flavor: m1.tiny
      network: public1
```

Figure 6.2 Ansible sample code SQL Injection Scenario

6.3 Detect Malicious Network Traffic

The objective of this cybersecurity exercise is to verify the availability and functionality of Zeek, Rita, and Tshark at Uniwa Cyber Range System. Additionally, participants will analyze

a provided PCAP file to accomplish tasks such as displaying capture duration, finding the SHA256 hash of the PCAP file, detecting malicious Command and Control (C2) beacons using Rita, and identifying and recognizing Command and Control traffic.

Scenario: As a cybersecurity analyst, you have access to a Docker container equipped with Zeek, Rita, and Tshark. Your task is to assess the functionality of these tools within the Docker environment and analyze a PCAP file containing suspicious network traffic. The exercise involves verifying tool availability, performing basic PCAP file analysis, and detecting various types of malicious activities.

Tools/Resources Required: 1. Docker container with Zeek, Rita, and Tshark installed 2. Pre-recorded PCAP file containing network traffic

Exercise Steps:

1. Docker Environment Verification:
2. Display Capture Duration and Timestamps:
3. Find SHA256 Hash of Pcap File:
4. Detect Malicious Command and Control Beacons with Rita:
5. Identify HTTPS Command and Control Traffic:
6. Recognize Command and Control Traffic:

This cybersecurity exercise provides participants with an opportunity to verify the functionality of Zeek, Rita, and Tshark within a Docker container and analyze malicious network traffic. By completing tasks such as displaying capture duration, finding the SHA256 hash of the PCAP file, and detecting various types of malicious activities, participants can enhance their skills in network traffic analysis and threat detection within a controlled environment.

6.4 Host Discovery and Port Scanning

The objective of this cybersecurity exercise is to perform host discovery and port scanning using various protocols and techniques with the Nmap tool. Participants will scan the network

to identify active hosts using ARP, UDP, ICMP ECHO, etc. Additionally, they will conduct port scans using TCP connect, Xmas, ACK flag probe, etc, followed by an analysis of the findings.

Scenario: As a cybersecurity analyst in Uniwa Cyber Range, you have been tasked with conducting host discovery and port scanning to assess the security posture of the network. Using Nmap, you will perform different types of scans to identify active hosts and open ports/services. The exercise aims to enhance your understanding of network reconnaissance techniques and their security implications.

Tools/Resources Required:

Nmap tool (pre-installed in Uniwa Cyber Range environment)

Exercise Steps:

1. Host Discovery: a. Perform a host discovery scan using ARP protocol with Nmap to identify active hosts on the network. b. Conduct a UDP packet scan to discover active hosts that may not respond to ARP requests. c. Use ICMP ECHO scan to detect active hosts by sending ICMP echo requests. d. Perform a TCP-ACK scanning to discover hosts that may not respond to ICMP or ARP. e. Execute an ICMP Address Mask Ping Scan to discover active hosts using ICMP address mask requests. f. Analyze the results of each scan to identify the discovered hosts and their status.
2. Port Scanning: a. Perform a TCP connect/full open scan to identify open ports and services on the discovered hosts. b. Conduct a stealth scan/TCP half-open to perform port scanning without establishing a full connection. c. Execute an Xmas scan to probe for open ports by setting specific TCP flags. d. Perform a TCP Maimon scan to detect open ports by exploiting the behavior of certain TCP stacks. e. Execute an ACK flag probe scan to identify filtered ports by sending ACK packets. f. Conduct a UDP scan to identify open UDP ports and associated services. g. Perform an SCTP COOKIE ECHO Scan to identify open SCTP ports. h. Analyze the findings from each port scan to identify open ports, services, and potential vulnerabilities.

3. Analysis and Reporting:
 - a. Compare the results of different host discovery techniques to identify any inconsistencies or discrepancies.
 - b. Analyze the findings from port scanning to identify potential security risks, such as open ports/services that could be exploited by attackers.
 - c. Document the discovered hosts, open ports/services, and any anomalies observed during the scans.
 - d. Provide recommendations for improving network security based on the analysis and findings.

Conclusion: This cybersecurity exercise provides participants with practical experience in host discovery and port scanning using Nmap, covering various protocols and scanning techniques. By analyzing the findings, participants can gain insights into the network's security posture and potential vulnerabilities, enabling them to implement appropriate measures to enhance security and mitigate risks.

6.5 Advanced Scanning Techniques

The objective of this cybersecurity exercise is to demonstrate advanced evasion techniques against Intrusion Detection Systems (IDS) and firewalls using the Nmap tool. Participants will learn how to utilize advanced scanning options to bypass network security measures and avoid detection by employing techniques such as packet fragmentation, IP address spoofing, and more.

Scenario: As cybersecurity analysts, you are tasked with assessing the effectiveness of your organization's network defenses against sophisticated attack techniques. Your objective is to conduct a series of Nmap scans utilizing evasion techniques to probe for weaknesses in the IDS and firewall systems. By simulating real-world attack scenarios, you will identify potential gaps in the network security posture and recommend strategies for improvement.

Tools/Resources Required:

Nmap tool (installed in the testing environment) Access to a network with IDS/firewall protection

6.6 Docker Container Vulnerability Scanning

The following exercise conducts vulnerability scanning on a Docker container image using Trivy and Gype tools to identify potential security risks and vulnerabilities.

Tools Used:

Trivy Gype

Materials Required:

Ensure that Docker, Trivy, and Gype tools are installed on your system. Obtain a Docker container image for scanning. You can either pull an image from a registry or use a locally available one.

1. Vulnerability Scanning with Trivy: Analyze the Trivy scan results to identify any high, medium, or low severity vulnerabilities present in the container image.
2. Vulnerability Scanning with Gype:

Review the Gype scan results to identify additional vulnerabilities detected in the container image.
3. Compare the results obtained from Trivy and Gype scans. Evaluate the effectiveness of each tool in identifying vulnerabilities and providing actionable insights. Consider factors such as coverage, accuracy, ease of use, and additional features offered by each tool.
4. Based on the vulnerabilities identified by both tools, devise a plan for remediation. Determine whether patches, updates, or configuration changes are necessary to mitigate the identified vulnerabilities.
5. Document the findings from both Trivy and Gype scans, including the comparison of results.
6. Prepare a comprehensive report detailing the vulnerability assessment process, identified risks, remediation steps, and insights gained from comparing the two tools.

Conclusion: By conducting vulnerability scanning with Trivy and Grype and comparing the results obtained, organizations can gain valuable insights into the security posture of their containerized environments. This exercise highlights the importance of leveraging multiple tools and techniques for comprehensive vulnerability management and risk mitigation.

6.7 Vulnerability Assessment with WackoPicko

To conduct a Vulnerability Assessment (VA) using the vulnerable web application WackoPicko to identify security weaknesses and potential exploits.

Tools Required are WackoPicko (Vulnerable Web Application), Burp Suite or OWASP ZAP

1. Discovery Phase: Begin by exploring the WackoPicko web application to understand its functionalities and features. Identify the different components, such as login pages, forms, input fields, and functionalities that may be vulnerable to security flaws.
2. Vulnerability Scanning: Utilize automated vulnerability scanning tools such as Burp Suite or OWASP ZAP to scan the WackoPicko application for common vulnerabilities like Cross-Site Scripting (XSS), SQL Injection, Directory Traversal, etc.
3. Testing using skipfish, w3af and compare the result :
4. Exploitation Phase: Attempt to exploit the identified vulnerabilities to gain unauthorized access or execute malicious actions within the WackoPicko application.
5. Analysis and Documentation: Document the findings of the Vulnerability Assessment, including the identified vulnerabilities, their severity levels, and potential impacts.

Conclusion: By conducting a Vulnerability Assessment using WackoPicko, participants can gain practical experience in identifying and exploiting security weaknesses commonly found in web applications. This exercise highlights the importance of regular security assessments to proactively identify and address vulnerabilities before they can be exploited by malicious actors.

Additionally, in the web security scenarios portfolio of the UNIWA Cyber Range, we aim to create a set of tools such as OWASP Broken Web Applications Project (a collection of vulnerable web applications), OWASP Security Shepherd, DVWA, bWAPP, and other applications/suites for learning and improving web security expertise.

Furthermore, we will examine tools such as BurpSuite, OWASP ZAP, and w3af, to discover and attack vulnerable services, and security flaws such as SQL injection, XSS, CSRF, and HTML injection [187].

6.8 Conclusion

In this Chapter a detailed examination of the use case scenarios is provided, demonstrating the practical applications and benefits of the proposed Cyber Range (CR) system. Through a series of exercises, this chapter has showcased the system's ability to simulate realistic cybersecurity challenges, offering participants invaluable hands-on training. The diverse scenarios highlight the system's flexibility and effectiveness in addressing various aspects of cybersecurity training. From basic security measures to advanced threat detection, each scenario is crafted to enhance participants' practical skills and knowledge, preparing them for real-world cyber threats. The comparative analysis with existing CR systems has further emphasized the unique strengths of the proposed system, particularly in terms of realism, adaptability, and comprehensiveness. These attributes make it a powerful tool for both education and research in the field of cybersecurity.

Chapter 7

Evaluation

This chapter aims to provide an in-depth analysis of the Cyber Range's effectiveness, usability, and overall impact on participants, particularly focusing on the feedback obtained from the UNIWA students who engaged with the platform. The evaluation process included rigorous testing scenarios to simulate real-world conditions, thereby assessing the system's performance under stress. These scenarios were designed to identify both the strengths and potential areas for improvement within the Cyber Range. The primary focus was on analyzing the system's capacity to handle intense usage while maintaining optimal performance, usability, and reliability. Feedback from students highlighted several key areas. While the overall performance of the Cyber Range was deemed satisfactory, there were observations regarding the user interface. The analysis also extended to the technical performance of the Cyber Range, using tools to measure CPU, RAM usage, and execution times across various scenarios. This evaluation helped in identifying bottlenecks and resource utilization patterns, providing a clear roadmap for enhancing system performance through better resource management.

Furthermore, the chapter discusses the students' overall satisfaction and the perceived value of the Cyber Range in their educational experience. The overwhelmingly positive feedback underscores the Cyber Range's effectiveness in providing practical cybersecurity training, thus affirming its role as a critical tool in cybersecurity education.

7.1 Analyzing System Performance through Stress Testing Scenarios

We conducted stress tests/scenarios to analyze the performance characteristics of the ETHACA Cyber Range using the dstat performance tool. In the following sections, we will introduce these stress tests and present the results of our experiments.

To evaluate the impact of running instances on the environment, we performed measurements. The parameters analyzed encompassed CPU, RAM usage, and execution time to running scenario environment. For this evaluation, we incrementally added a node instance each time to facilitate the analysis process. Yaml code is depicted in Figure 7.1.

<pre> 4 parameters: 5 external_network: 6 type: string 7 default: public1 8 internal_network: 9 type: string 10 default: demo-net 11 resources: 12 secgroup: 13 type: OS::Neutron::SecurityGroup 14 properties: 15 name: sg_group 16 description: ssh, security group 17 rules: 18 - protocol: tcp 19 port_range_min: 22 20 port_range_max: 22 21 22 srv01: 23 type: OS::Zun::Container 24 properties: 25 image: "cirros:latest" 26 environment: 27 security_groups: 28 - {get_resource: secgroup} 29 networks: 30 - network: {get_param: external_network} 31 32 srv02: 33 type: OS::Zun::Container 34 properties: 35 image: "cirros:latest" 36 environment: 37 security_groups: 38 - {get_resource: secgroup} 39 networks: 40 - network: {get_param: external_network} </pre>	<pre> 1 parameters: 2 key_name: 3 type: string 4 default: keyserver 5 node_count: 6 type: number 7 label: Number of VM instance 8 description: Number of VM instance 9 default: 10 10 node_image: 11 type: string 12 label: Image ID 13 description: OS of VM instances 14 default: cirros 15 node_flavor: 16 type: string 17 default: m1.tiny 18 private_net: 19 type: string 20 default: demo 21 resources: 22 nodes: 23 type: OS::Heat::ResourceGroup 24 properties: 25 count: { get_param: node_count } 26 resource_def: 27 type: OS::Nova::Server 28 </pre>
Container yaml code	VM yaml code

Figure 7.1 Container and VM performance sample code

Experimental Results

Our analysis of the Cyber Range's performance revealed valuable insights. We observed the CPU utilization patterns during workload scenarios, enabling us to optimize resource

Table 7.1 Resources consumption by running ISO instances of ETHACA Cyber Range.

No of Instances	Max CPU usage [%]	Max RAM usage in MBytes	Execution time in seconds
1	21	222	17
2	26	443	25
4	33	1953	41
8	54	4871	54
10	64	6269	77

Table 7.2 Resources consumption by running container instances of ETHACA Cyber Range.

No of Instances	Max CPU usage [%]	Max RAM usage in MBytes	Execution time in seconds
1	13	40	9
2	16	40	9
4	20	78	16
8	25	90	16
10	29	93	16

Table 7.3 Capacity of compute, memory and storage of VM.

Flavor	VCPUs	Disk (in GB)	RAM (in MB)
m1.tiny	1	1	512

allocation and prevent performance degradation. Memory consumption analysis helped identify memory-related issues and implement effective memory management practices. The examination of execution time aided in identifying and resolving operation speed measurements within the Cyber Range.

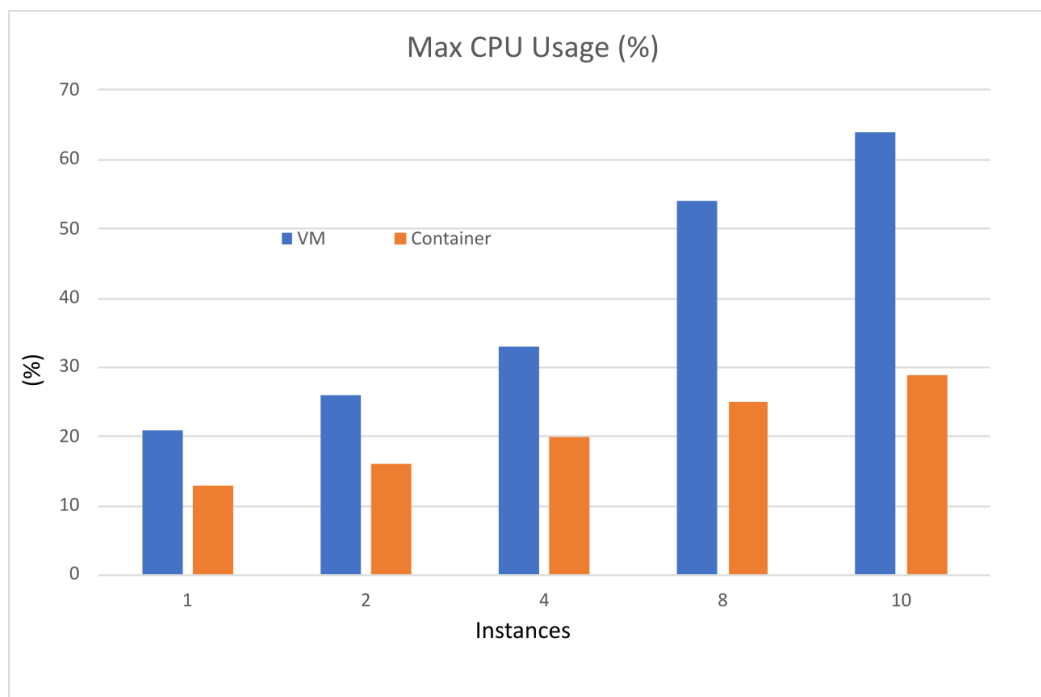


Figure 7.2 CPU Performance Comparison

The performance analysis of the ETHACA Cyber Range using the dstat tool provided a comprehensive understanding of its performance characteristics. The stress tests focused on CPU utilization, memory consumption, and execution time is illustrated in Figure 7.2, 7.3 and 7.4 allowing us to identify areas for optimization and enhance the Cyber Range's overall performance.

Based on the information presented in Tables 7.1 and 7.2, it is evident that increasing the resources utilized in the scenarios results in only a slight increase in computational resources and implementation time when using container technology. However, when employing VMs, there is an exponential increase in both computational resources and implementation time. The VM resources that are used in the instance are presented in Table 7.3.

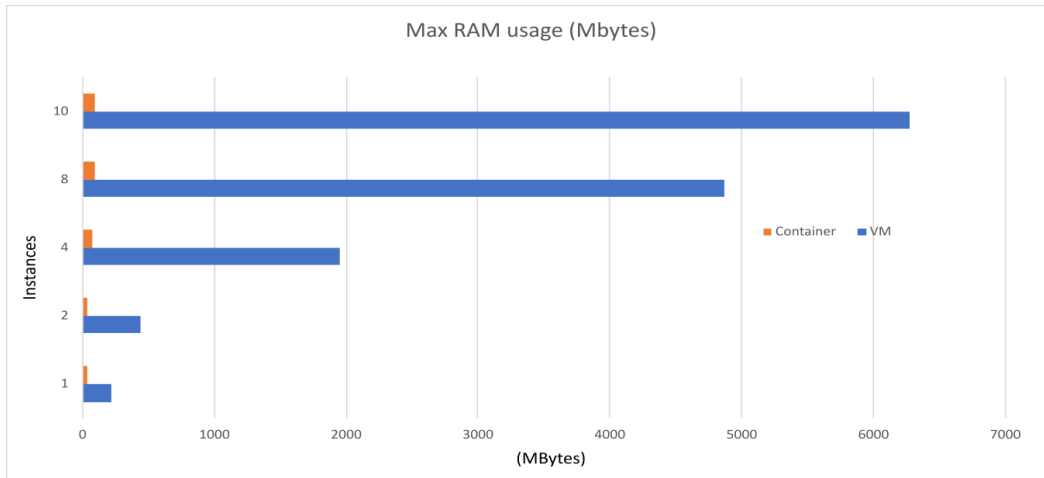


Figure 7.3 Memory Performance Comparison

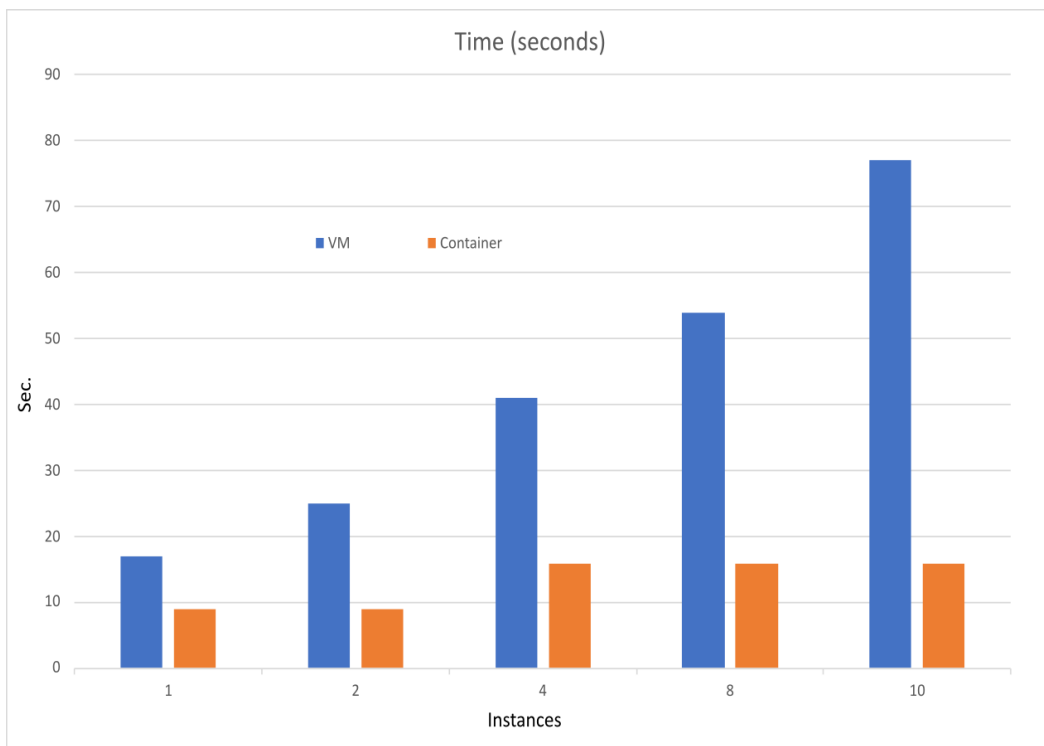


Figure 7.4 Execution Time Comparison

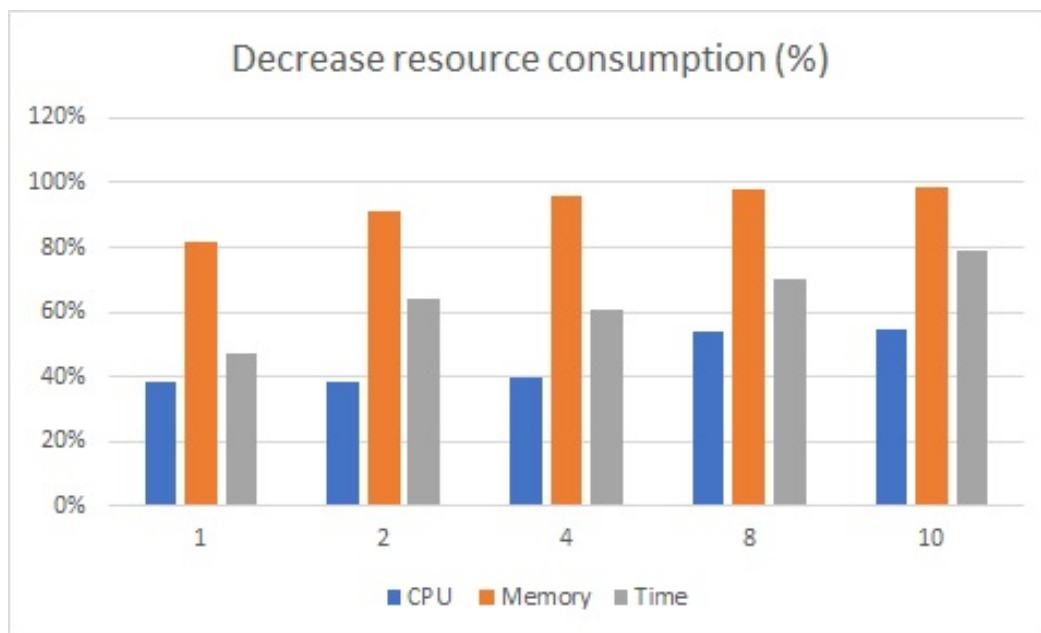


Figure 7.5 Decrease resource consumption VM vs Container (%)

Furthermore, as depicted in Figure 7.5, the use of containers leads to significant savings in implementation time, with a reduction of approximately 79%. Moreover, containerization achieves over 90% reduction in memory usage and 50% reduction in CPU utilization. It is important to note that these percentages are estimated, and actual values may vary depending on the realism of the scenarios being executed.

Overall, the findings demonstrate that container technology offers notable advantages over VMs in terms of resource efficiency and implementation time. By leveraging containers in the ETHACA Cyber Range, we can optimize resource allocation and achieve efficient execution of scenarios.

7.2 User Acceptance

The research was carried out at the University of West Attica. The presentation of the ETHACA Cyber Range was organized over two separate days. This event was primarily attended by security experts and students members of the Information, Network, and System Security (INSSec) research team, postgraduates, and as well as students from the undergradu-

ate course in Information Technology Security. The presentation began with a comprehensive analysis of the design and implementation of ETHACA Cyber Range, providing detailed insights into its architecture and operational capabilities. Attendees were introduced to the strategic planning and technical intricacies involved in setting up the Cyber Range, which serves as a simulated environment for testing and improving cybersecurity measures.

Following the theoretical overview, a practical demonstration of a cyber security exercise was conducted. This included showcasing exercises that have been previously developed within the Cyber Range framework. These exercises are designed to emulate real-world cyber-attack scenarios, allowing participants to apply their knowledge and skills in a controlled environment. Participants were then given specific exercises to solve, offering them hands-on experience with cyber security challenges. These exercises aimed to enhance their understanding of cyber threats and the corresponding defensive strategies, providing a valuable learning opportunity.

After the event, a questionnaire was distributed to all participants. This feedback mechanism was intended to gather insights on the effectiveness of the cyber range demonstration and the overall learning experience, ensuring continuous improvement of the program. The questionnaire was designed to capture information, including prior experience in cybersecurity, preferences for cybersecurity training categories, and specific feedback on ETHACA.

7.2.1 Data from the survey

Years Involved in Cybersecurity

Participants were asked to specify their years of experience in cybersecurity, categorized into several ranges: 0-1 years, 2-4 years, 5-6 years, 7-9 years, 10+ years, 15+ years, and Other. This data helped in understanding the diversity within the participant group and in correlating experience levels with the feedback provided. The analysis aimed to identify trends and differences in responses based on varying levels of experience.

Participation in Cybersecurity Exercises

The questionnaire included questions about participants' prior involvement in cybersecurity exercises. This data was analyzed to assess the proportion of participants familiar with such exercises. High participation rates would indicate a well-prepared group, whereas low rates might suggest the need for introductory resources to enhance readiness and understanding.

Types of Cybersecurity Exercises

Participants were asked to identify the types of exercises they had previously engaged in, such as Capture The Flag (CTF), Tabletop Exercises, Red/Blue Team Exercises, Cyber Range Exercises, and Other. Understanding the variety of exercises participants were familiar with helped tailor the Cyber Range activities to better suit their prior experiences and broaden their skill sets.

Previous Engagement with Cyber Ranges

Questions regarding prior use of Cyber Ranges aimed to gauge participants' expectations and relevance of their feedback. Analyzing this data provided insights into how the ETHACA Cyber Range compared with other Cyber Ranges participants might have experienced.

Desired Cybersecurity Categories

Participants indicated their interest in various cybersecurity categories, including Web Security, Network Security, Software Security, System Security, Social Engineering, Threat Intelligence, Cryptography, and Red/Blue Team. Analyzing these preferences helped ensure the Cyber Range's curriculum was aligned with participants' needs and interests, facilitating targeted skill development.

Experience with ETHACA Cyber Range

Participants' experiences with the ETHACA Cyber Range were evaluated across several key criteria. The development of advanced skills was assessed by measuring participants' agree-

ment on how effectively the Cyber Range facilitated deeper learning beyond basic concepts. The knowledge of infrastructure components was evaluated to understand improvements in understanding servers, storage systems, and cloud technologies. Network creation and security knowledge were assessed to determine if the range advanced participants' abilities in network security protocols and management practices. The impact on programming and software development knowledge was measured by evaluating gains in secure coding, software vulnerability understanding, and security implementation skills. Lastly, the efficiency in creating cybersecurity exercises was analyzed, focusing on how well the Cyber Range supported the design and implementation of training exercises. Data from these evaluations provided insights into the strengths and areas for improvement, guiding future enhancements to better meet the diverse needs of users and support advanced cybersecurity training.

Importance of Incorporating a Cyber Range

Participants rated the importance of incorporating a Cyber Range in their training. This helped gauge overall sentiment towards the Cyber Range's role in enhancing technical knowledge and its perceived value in cybersecurity education.

Additional Features or Capabilities

Participants were invited to suggest additional features or improvements that could enhance the Cyber Range. This qualitative feedback was crucial for identifying potential enhancements that would make the Cyber Range more useful for educational or research purposes.

Assessment of Working Environment

Satisfaction with the working environment was measured from "Very Satisfied" to "Very Dissatisfied." This feedback aimed to identify areas needing improvement to ensure a conducive and productive training environment.

Overall Helpfulness

Participants rated the overall helpfulness of their experience at ETHACA from "Extremely Helpful" to "Extremely Unhelpful." This provided a holistic view of participant satisfaction and the effectiveness of the Cyber Range in achieving its educational objectives.

7.2.2 Results

This study evaluates participants' perceptions of the ETHACA Cyber Range system to understand its effectiveness in fostering practical cybersecurity knowledge and skills. By analyzing responses from a comprehensive questionnaire, we can assess the system's impact on participants' learning experiences and identify areas for improvement. The questionnaire covered various aspects, including participants' experience in cybersecurity, their engagement with different types of exercises, and their specific needs and satisfaction with the ETHACA Cyber Range.

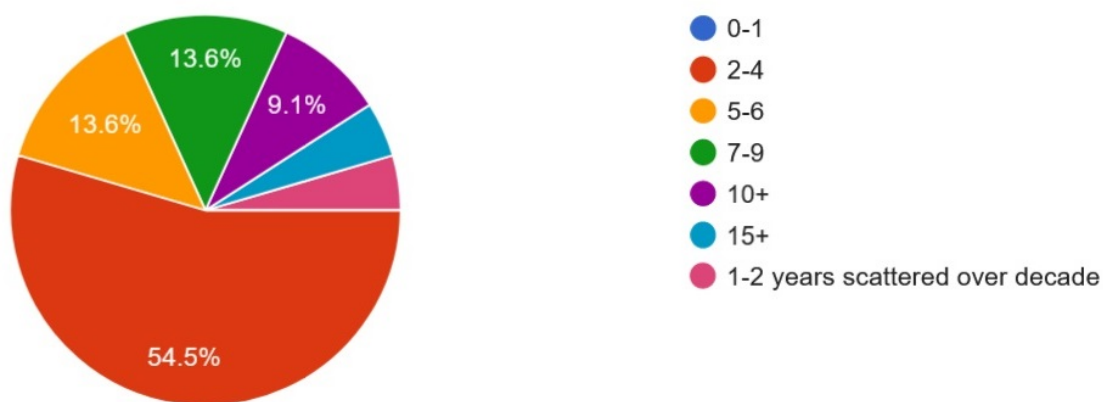


Figure 7.6 Years Involved in Cybersecurity

Years Involved in Cybersecurity

The participants' experience in cybersecurity varied widely as depicted in figure 7.6, with the majority (55%) having 2-4 years of experience. This group was followed by those with 5-6 years and 7-9 years (14%), 10+ years (9%), 0-1 years and 15+ (4%). The data gathered from this question serves to assess the participants' level of expertise in the cybersecurity

domain. The fact that 41% of the participants have over 5 years of experience indicates a substantial presence of seasoned professionals within the cohort. This suggests a high level of specialized knowledge and a deep understanding of the complexities associated with cybersecurity, contributing to the overall credibility and depth of the study's findings.

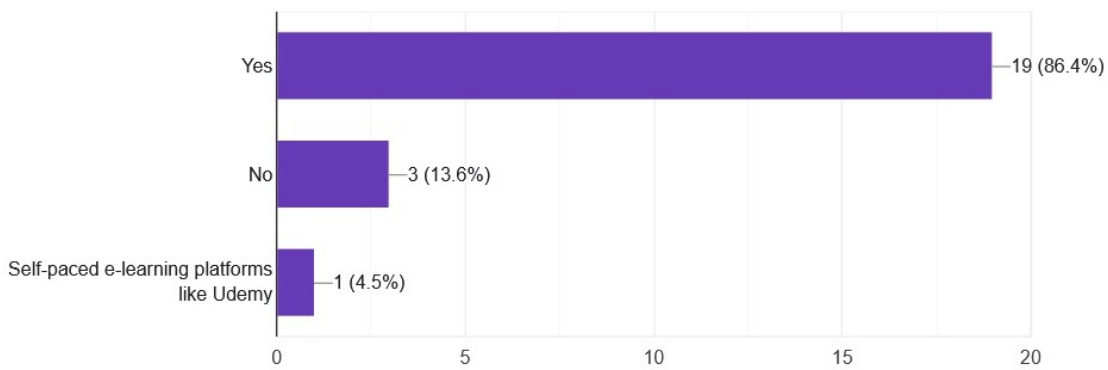


Figure 7.7 Participation in Cybersecurity Exercises

Participation in Cybersecurity Exercises

As depicted in figure 7.7 a significant proportion of participants (86%) reported having previously engaged in cybersecurity exercises. This high level of prior engagement underscores a foundational familiarity with cybersecurity training environments among the user base. Such prior exposure is likely to enhance participants' ability to engage in more complex and substantive interactions within the Cyber Range, thereby contributing to the overall effectiveness and depth of the training experience. This pre-existing knowledge base may also serve as a critical enabler for more nuanced learning outcomes and a greater capacity for participants to tackle sophisticated cybersecurity scenarios.

Types of Cybersecurity Exercises Participated In

Among those with prior exercise experience, Red/Blue Team activities was the most common (50%), followed by Capture The Flag (CTF) (45%), Table Top exercises and Cyber Range exercises (20%) as shown in figure 7.8. This distribution indicates a distinct inclination towards interactive and competitive formats. The prominence of these formats underscores

the critical importance of integrating similar interactive elements within the Cyber Range environment to sustain user engagement and effectively emulate real-world cybersecurity scenarios.

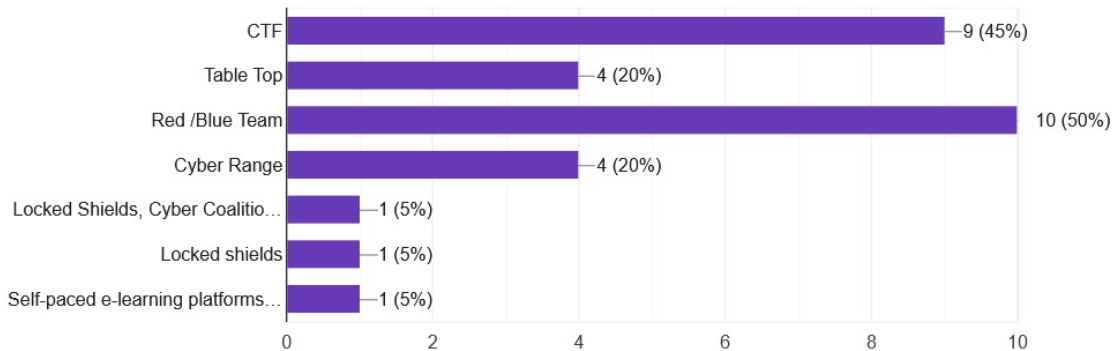


Figure 7.8 Types of Cybersecurity Exercises Participated In

Previous Engagement with Cyber Ranges

Nearly half of the participants (45%) had previous experience with Cyber Ranges as illustrated in figure 7.9, suggesting that while many users are familiar with such platforms, there is still a significant portion (55%) for whom the ETHACA Cyber Range might be their first exposure. This proportion highlights the importance of designing a user interface that is not only intuitive but also supplemented with comprehensive introductory resources. Such an approach is essential to cater to the diverse needs of both novice and experienced users, ensuring effective engagement and maximizing the platform's accessibility and usability.

Desired Cybersecurity Categories

Participants expressed a strong interest in Web Security (64%), Network Security (59%), and Software Security (55%) as shown in figure 7.10, reflecting a demand for practical, hands-on learning in these critical areas. This distribution of preferences underscores a considerable demand for experiential, hands-on learning opportunities in these pivotal domains. The feedback collected thus emphasizes the imperative to align curriculum development with these areas of focus to effectively address both participant expectations and evolving industry requirements.

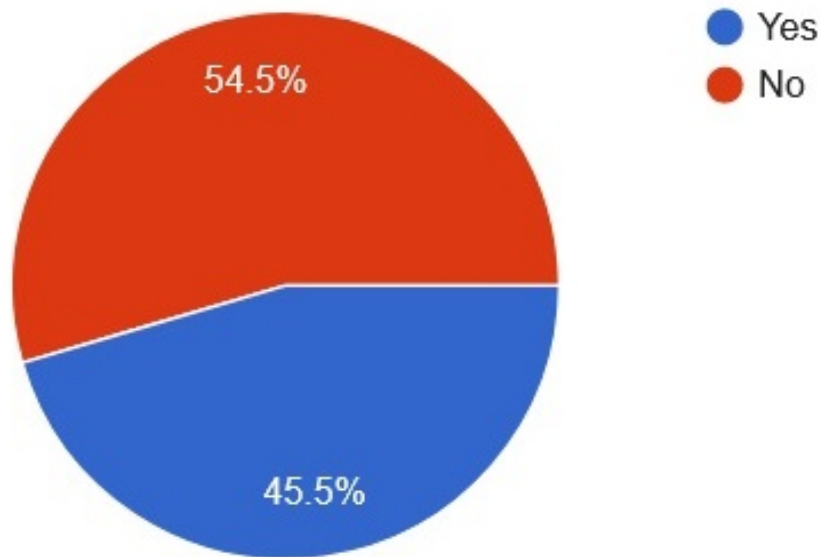


Figure 7.9 Previous Engagement with Cyber Range

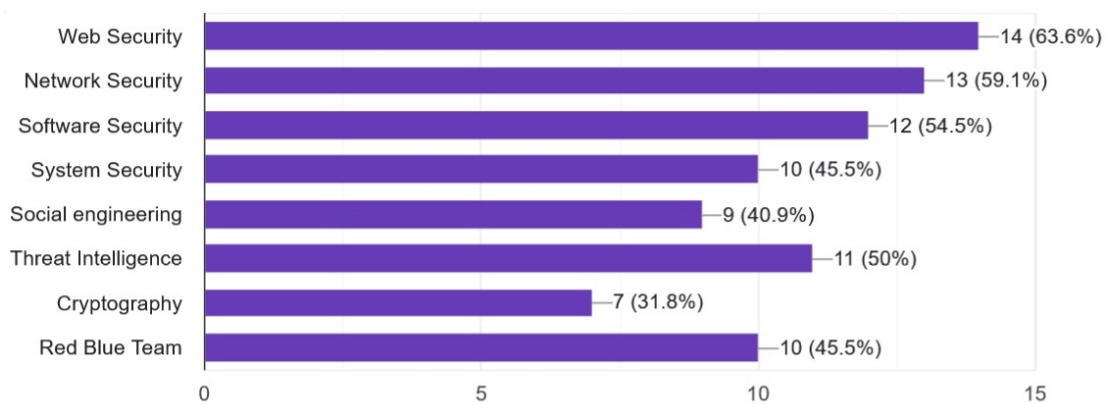


Figure 7.10 Desired Cybersecurity Categories

Experience with ETHACA Cyber Range

As illustrated in figure 7.11, participants' feedback on the ETHACA Cyber Range highlights its effectiveness in several key areas. Specifically, 59% of respondents strongly agreed, and 36% agreed that the Cyber Range significantly contributes to the development of advanced cybersecurity skills and strategies. This strong positive response indicates that the Cyber Range successfully provides complex, hands-on exercises that enhance participants' practical skills. Additionally, 42% of participants strongly agreed and another 45% agreed that the Cyber Range expands their knowledge of infrastructure components such as servers, storage, and cloud services, demonstrating its comprehensive coverage of essential technical areas. In terms of network security, an equal 32% strongly agreed and 45% agreed that the Cyber Range advances their knowledge in network creation, management, and security, which underscores its effectiveness in teaching critical networking concepts. However, the responses were more varied regarding programming and software development; 27% agreed, while 45% neither agreed nor disagreed, suggesting that while the Cyber Range is beneficial in many areas, it may need to improve its offerings related to programming and software development to better meet the needs of all participants. Lastly, 40% strongly agreed and 45% agreed that the Cyber Range streamlines the process of creating cybersecurity exercises, indicating that it provides efficient tools and resources for exercise development, thus reducing the time and effort required for such tasks.

Importance of Incorporating a Cyber Range

A significant majority of respondents 57% identified the integration of a Cyber Range into the curriculum as important, with an additional 33% considering it to be very important as shown in figure 7.12. This strong endorsement underscores the essential role that practical cybersecurity training tools play in enhancing students' technical proficiency. Moreover, it highlights the importance of preparing students to effectively address the complex challenges they will face in their professional careers. The findings reflect a clear consensus on the value of hands-on learning environments, such as Cyber Ranges, in cultivating a deeper and more applied understanding of cybersecurity.

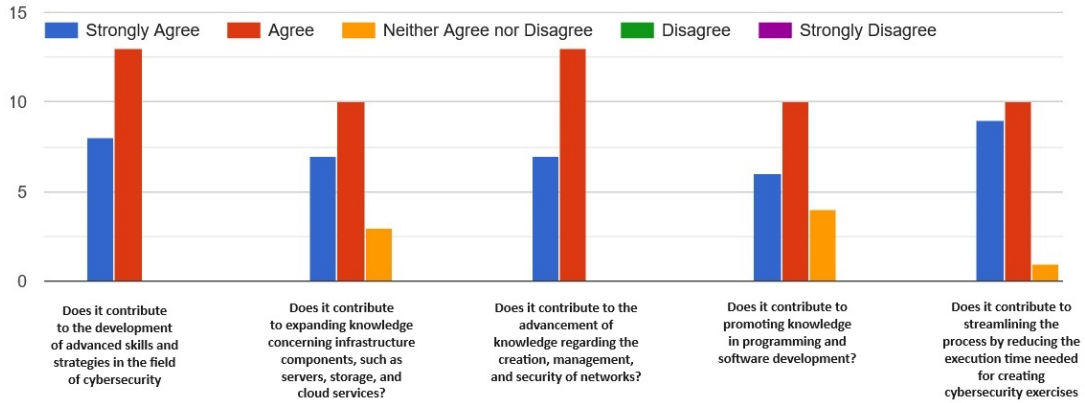


Figure 7.11 Experience with ETHACA Cyber Range

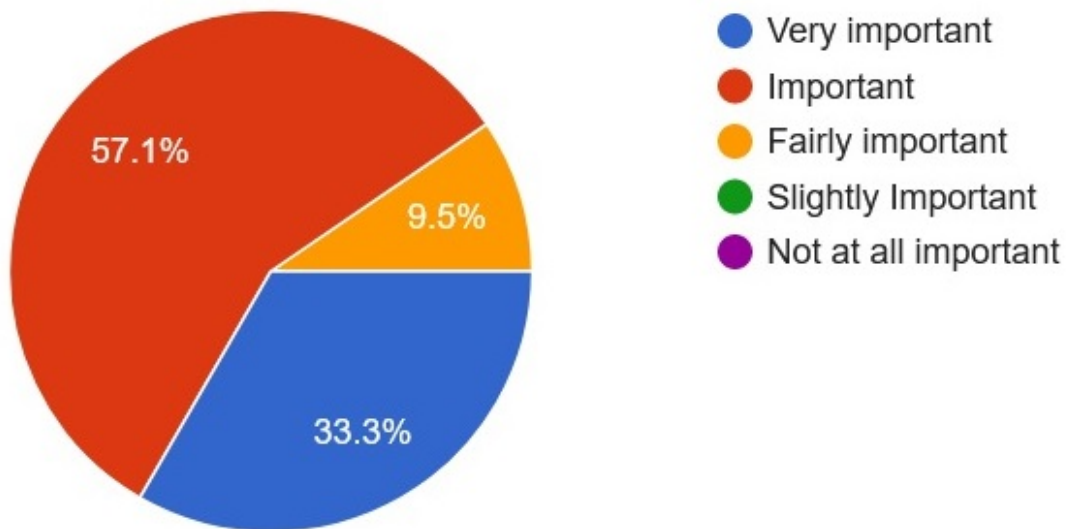


Figure 7.12 Importance of Incorporating a Cyber Range

Additional Features or Capabilities

Participants have identified several potential enhancements to the Cyber Range, including the integration of advanced threat hunting exercises, expanded security awareness modules, artificial intelligence-driven scenarios, and detailed tutorials. These suggestions underscore a collective aspiration for a more immersive and comprehensive educational environment, one that is capable of simulating intricate and realistic cybersecurity challenges. Such developments would significantly augment the Cyber Range's capacity to offer a more robust and holistic learning experience, thereby better equipping participants to navigate the complexities of contemporary cybersecurity landscapes.

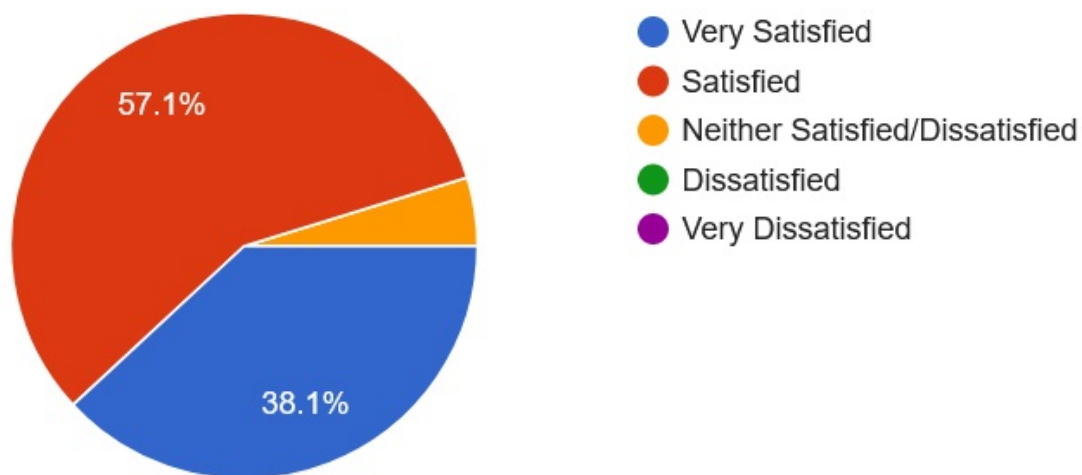


Figure 7.13 Assessment of Working Environment

Assessment of Working Environment

The ETHACA Cyber Range working environment received largely positive evaluations, as illustrated in Figure 7.13. Notably, 38% of participants indicated they were very satisfied, and an additional 57% reported being satisfied. This positive feedback reflects a well-designed and supportive learning environment. However, there is still room for further improvement to enhance overall satisfaction and address any areas that may require attention to ensure a consistently high-quality experience for all participants.

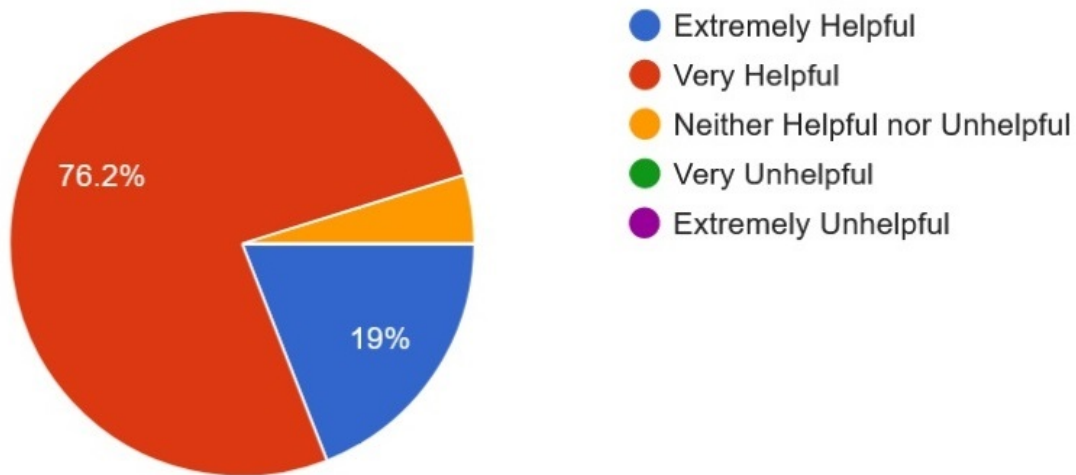


Figure 7.14 Overall Helpfulness

Overall Helpfulness

Overall, the ETHACA Cyber Range was deemed extremely helpful by 19% of respondents and very helpful by 76% as illustrated in figure 7.14. This overwhelmingly positive assessment demonstrates the system's effectiveness in providing valuable cybersecurity training and education, supporting its continued use and development as a key educational tool.

7.3 Conclusion

We proposed ETHACA Cyber Range as a highly effective platform, well-regarded by participants for its ability to develop critical skills and knowledge. To address the reported usability issues, developing an improved web service with enhanced user-friendly features is recommended for the next version of the ETHACA Cyber Range. This would enhance the overall accessibility and navigation experience within the ETHACA Cyber Range platform. To minimize scenario implementation delays, a thorough assessment of resource allocation should be conducted. This evaluation should explore allocating additional resources to ensure optimal performance. The high level of previous engagement in cybersecurity exercises and the significant number of users with prior Cyber Range experience indicates a strong foundation of familiarity, which enhances the efficacy of the training provided. The evaluation

of the ETHACA Cyber Range through participant feedback reveals a robust and effective platform for conducting cybersecurity exercises. The diversity of experience levels among participants suggests that the Cyber Range is accessible and beneficial to both novice and experienced users. Participants expressed a clear preference for network and web security, as well as Red/Blue Team exercises, highlighting the need for the Cyber Range to focus on these critical areas. Furthermore, the strong consensus on the importance of integrating the Cyber Range into the curriculum reflects its perceived value in enhancing technical cybersecurity knowledge. ETHACA Cyber Range has demonstrated significant effectiveness in developing advanced cybersecurity skills, yet there are areas for enhancement that can propel it to new heights of educational excellence. One critical area for future development is the expansion of programming and software development modules. User experience improvements should be a continuous focus. Refining the user interface to ensure it is intuitive and user-friendly can significantly enhance the learning experience.

Additionally, implementing personalized learning paths that adapt to the user's skill level and progress can provide a tailored educational journey, maximizing the effectiveness of the Cyber Range. Incorporating emerging technologies such as AI, machine learning, and IoT security into the curriculum will ensure that the Cyber Range remains at the cutting edge of cybersecurity education. These technologies are becoming increasingly important, and providing users with knowledge and skills in these areas will prepare them for the future landscape of cybersecurity.

Chapter 8

Conclusion and Future Work

This thesis addresses the evolution, challenges, and future directions of Cyber Range systems in the context of cybersecurity education and research. It incorporates insights from an extensive review of current Cyber Range systems and structured interviews with industry experts, revealing the critical importance of scalability, adaptability, and seamless integration with educational frameworks. The comparative analysis of contemporary architectures and platforms, along with detailed case studies, highlights the advantages of innovative container-based solutions in providing interactive and practical cybersecurity training. Evaluations of user acceptance underscore the platform's effectiveness in enhancing cybersecurity skills, while future directions suggest improvements in scalability, flexibility, and the integration of emerging technologies. This thesis aims to significantly contribute to the ongoing development and refinement of Cyber Range systems, ensuring their continued relevance and effectiveness in addressing the sophisticated landscape of cyber threats.

8.1 Conclusions

8.1.1 Current State-of-the-Art Regarding Testbeds and Cyber Ranges

The comprehensive literature review and structured interviews conducted in this study provide a nuanced understanding of the current state-of-the-art Cyber Range systems. The analysis

revealed a diverse array of Cyber Ranges, each tailored to specific objectives, sectors, and types of environments. For instance, the NATO Cyber Range [36] emphasizes large-scale, realistic military exercises, while Masaryk University's KYPO [131] focuses on academic and research applications, providing flexible and scalable training environments.

The structured interviews with technical directors and managers of Cyber Ranges yielded valuable insights into the operational challenges and benefits of these systems. Interviewees highlighted the critical importance of scalability and adaptability in Cyber Range design. For example, they noted the need for systems that can accommodate increasing numbers of users and simulate complex cyber ecosystems. Additionally, the ability to integrate seamlessly with existing educational frameworks and technological infrastructures was identified as a key factor in the effective deployment and utilization of Cyber Ranges. These insights underscore the necessity of developing Cyber Ranges that are not only technologically advanced but also user-friendly and easily integrated into diverse operational contexts.

8.1.2 Contemporary Architectures and Comparative Analysis

The detailed examination of contemporary Cyber Range architectures revealed significant advancements in scalability, flexibility, and resource management. Modern Cyber Ranges, such as the ETHACA Cyber Range, have adopted container-based architectures, which offer modularity and efficiency. These systems leverage cutting-edge virtualization and orchestration tools to create flexible and scalable environments that can simulate a wide range of cyber threats and scenarios.

The comparative analysis of various platforms highlighted notable differences in performance, cost, and scalability. For instance, OpenStack was identified as a particularly advantageous platform due to its robust support for scalability and seamless integration capabilities. The analysis showed that while some platforms excel in specific areas, a comprehensive solution requires balancing multiple factors to achieve optimal performance and usability. Visual summaries and comparative tables were used to elucidate these findings, providing a clear and accessible overview of the strengths and weaknesses of different Cyber Range platforms.

8.1.3 Introducing a Novel Container-Based Cyber Range Architecture

The introduction of a novel container-based Cyber Range architecture addresses several critical limitations of existing systems. This architecture is designed to be highly scalable and adaptable, utilizing a modular approach that facilitates easy updates and modifications. The use of containerization technologies, such as Docker, allows for the efficient allocation of resources and supports a wide range of simulation scenarios.

The detailed design and implementation process involved the development of six constituent modules, each playing a crucial role in the overall architecture. These modules include the Web Fronted, Storage, Scenario, Management, Environment, and Orchestration. Each module is designed to enhance specific aspects of the Cyber Range, ensuring a comprehensive and effective training environment. Significant emphasis was placed on the advantages of open-source cloud platforms. Platforms like Docker and OpenStack offer cost-effectiveness, flexibility, and strong community support, making them ideal choices for developing robust Cyber Ranges. The practical benefits of these technologies were demonstrated through case studies and specific implementation examples, highlighting their impact on the efficiency and scalability of the proposed architecture.

8.1.4 Optimizing Cyber Range Implementation

The implementation of the proposed Cyber Range architecture centers on the strategic selection and deployment of infrastructure platforms and technologies, such as Docker and OpenStack. The process effectively demonstrated the architecture's practical viability, overcoming various deployment challenges and integrating advanced systems into existing technological frameworks. The enhancement of monitoring and alerting capabilities, played a crucial role in improving the system's effectiveness and responsiveness. These tools provided real-time monitoring and comprehensive analytics, which are essential for maintaining the operational integrity of the Cyber Range. The deployment of the Cyber Range underscored the importance of modern technologies in simplifying implementation

processes and increasing the system's capacity to deliver realistic and immersive training environments for cybersecurity education and research.

Furthermore, the work highlights the ongoing need for refinement and adaptation to emerging technologies, ensuring that the Cyber Range remains effective and relevant in the continually evolving cybersecurity landscape. The successful integration of these technologies demonstrates the system's robustness and its potential to significantly contribute to the field of cybersecurity training and research.

8.1.5 Bridging the Cybersecurity Skills Gap

The exploration of Cyber Ranges as a tool for enhancing cybersecurity competence reveals their critical role in bridging the gap between theoretical knowledge and practical application. Moreover, the utilization of Cyber Ranges in conjunction with well-designed cybersecurity exercises provides a robust platform for translating theoretical knowledge into real-world skills. This hands-on approach is essential for developing the practical expertise required to respond to the dynamic and evolving nature of cyber threats. The adaptability and immersive nature of Cyber Ranges make them particularly effective in preparing individuals for the complexities of modern cybersecurity challenges. The ongoing need for research into the long-term impacts of these training methodologies is highlighted, with an emphasis on continuous innovation in the design and implementation of cybersecurity training programs.

8.1.6 Presenting Use Case Scenarios

The practical application and effectiveness of the Cyber Range were illustrated through detailed use case scenarios. These scenarios covered a variety of common and advanced cybersecurity threats, including SQL injection vulnerabilities, advanced scanning techniques, and malicious network traffic detection. Each scenario was designed to provide participants with hands-on experience in identifying and mitigating cyber threats in a controlled, realistic environment. For example, the SQL injection scenario demonstrated the process of identifying and exploiting a vulnerability, followed by the implementation of mitigation strategies.

Participants were able to engage with the scenario interactively, gaining practical skills and insights that are directly applicable to real-world cybersecurity challenges. Summarizing the key outcomes and benefits of each use case scenario provided a clear and compelling illustration of the Cyber Range's capabilities and its value as a training tool.

8.1.7 User Acceptance and Effectiveness

Evaluations of user acceptance and effectiveness revealed high levels of satisfaction and significant improvements in participants' cybersecurity skills. Surveys and performance metrics indicated that a substantial majority of users experienced enhanced abilities in threat detection, response, and mitigation following their training on the ETHACA Cyber Range Platform. Key feedback from users emphasized the platform's intuitive interface, realistic simulation environments, and the practical relevance of the training scenarios. Testimonials from participants further validated the effectiveness of the platform, underscoring its role in providing high-quality, impactful cybersecurity training. Presenting these statistics and testimonials highlighted the platform's broad acceptance and its significant contributions to improving practical cybersecurity skills among users.

8.2 Future Directions

Cyber Ranges can be used to enhance realism, soft skills development, evaluation mechanisms, and incorporation of emerging technologies. By addressing these areas, Cyber Ranges can provide more effective and comprehensive training environments, better preparing cybersecurity professionals to tackle the evolving landscape of cyber threats. These directions are based on the gaps and challenges identified in the comprehensive literature review, ensuring that the proposed advancements are grounded in the current state-of-the-art and reflect the latest developments in cybersecurity training and research.

Cyber Range architectures should focus on integrating advanced telecommunication and IoT capabilities, including emulated banking systems, hospital networks, smart grids, automated vehicles, and virtual cyber operation centers, to provide realistic and comprehen-

sive training environments. The development of cloud-based Cyber Ranges will enhance accessibility and usability, facilitating broader collaboration and enabling detailed cybersecurity experiments. Transitioning to digital twin technology will improve the realism of training scenarios, while enhancements in real-time monitoring and visualization will aid in rapid threat identification and response. Implementing advanced authentication and privacy mechanisms will address security and data privacy concerns, ensuring secure access and protection of sensitive data. Leveraging open-source tools and fostering community collaboration through shared resources will promote innovation and continuous improvement in Cyber Range technologies, keeping them at the forefront of cybersecurity training and research.

Cyber Range implementation should concentrate on enhancing scalability, integration, security, user experience, and monitoring capabilities. Advanced container orchestration platforms are essential for dynamic scaling based on user demand, minimizing manual intervention. Deeper integration with diverse deployment technologies and frameworks will ensure smoother adoption and interoperability across various cybersecurity training and research activities. Incorporating automated threat detection and response systems will fortify security against emerging cyber threats. Improving the user experience through intuitive interfaces and comprehensive training modules will make the Cyber Range more accessible and effective for users with varying levels of expertise. Lastly, enhancing monitoring and alerting capabilities with real-time data collection and analysis tools will provide precise and actionable insights, thereby improving the overall effectiveness and responsiveness of the Cyber Range system. These strategic directions will significantly bolster the capacity and efficacy of Cyber Ranges in preparing cybersecurity professionals for real-world challenges.

Efforts should also focus on improving the accessibility and usability of Cyber Ranges to ensure that they can be effectively utilized by organizations of all sizes, including small and medium-sized enterprises (SMEs). This involves designing user-friendly interfaces and providing comprehensive support and documentation to facilitate the adoption and integration of Cyber Ranges into existing training programs. Additionally, exploring the incorporation of behavioral strategies and gamification techniques into cybersecurity training can significantly

enhance engagement and retention. Another critical area is the evaluation and validation of Cyber Range training effectiveness. Developing standardized assessment metrics and methodologies will enable more rigorous evaluation of training outcomes, helping to identify best practices and areas for improvement. Also, fostering collaboration between academia, industry, and government agencies can drive the development of more comprehensive and relevant cybersecurity training programs.

Enhancing cybersecurity training within the Cyber Range to cover emerging technologies and threats, such as IoT devices and industrial control systems (ICS), will maintain relevance in the evolving technological landscape. Incorporating advanced data analytics and reporting tools will provide real-time feedback and performance metrics, aiding participants in identifying strengths and areas for improvement. Lastly, fostering collaboration with industry partners to integrate best practices and real-world insights will enhance the realism and relevance of training scenarios, ensuring the Cyber Range remains at the forefront of cybersecurity education.

We propose several future enhancements and research directions based on participant feedback to further improve the ETHACA Cyber Range platform. These include expanding programming and software development modules, refining the user interface for better accessibility, and implementing personalized learning paths. Addressing these areas will ensure the ETHACA Cyber Range continues to evolve as a cutting-edge platform, preparing learners for the increasingly sophisticated cyber threat landscape.

Bibliography

- [1] Leandros Maglaras, George Drivas, Nestoras Chouliaras, Eerke Boiten, Costas Lambrou, and Sotiris Ioannidis. Cybersecurity in the era of digital transformation: the case of greece. In *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*, pages 1–5. IEEE, 2020.
- [2] ENISA. Cyber Europe 2022. <https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2022>, 2022. (last accessed: 22.12.2022).
- [3] Jan Vykopal, Pavel Čeleda, Pavel Seda, Valdemar Švábenský, and Daniel Tovarňák. Scalable learning environments for teaching cybersecurity hands-on. In *2021 IEEE Frontiers in Education Conference (FIE)*, pages 1–9. IEEE, 2021.
- [4] Falko Schönreich and Günther Pernul. Cyber range exercises: Potentials and open challenges for organizations.
- [5] Alexander A Zakharov, Shamil I Khanbekov, Irina G Zakharova, and Dmitriy A Korenev. Management of the cyber range functionality based on the analysis of the digital footprint of students. In *2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE)*, pages 920–924. IEEE, 2023.
- [6] Leandros A Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J Cruz. Cyber security of critical infrastructures. *ICT Express*, 4(1):42–45, 2018.
- [7] Mohamed Amine Ferrag. Epec: an efficient privacy-preserving energy consumption scheme for smart grid communications. *Telecommunication Systems*, 66(4):671–688, 2017.
- [8] Mohamed Amine Ferrag, Mehdi Nafa, and Salim Ghanemi. Epsa: an efficient and privacy-preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks. *International Journal of Security and Networks*, 11(3):107–125, 2016.
- [9] Chiara Braghin, Stelvio Cimato, Ernesto Damiani, Fulvio Frati, Lara Mauri, and Elvinia Riccobene. A model driven approach for cyber security scenarios deployment. In Apostolos P. Fournaris, Manos Athanatos, Konstantinos Lampropoulos, Sotiris Ioannidis, George Hatzivasilis, Ernesto Damiani, Habtamu Abie, Silvio Ranise, Luca Verderame, Alberto Siena, and Joaquin Garcia-Alfaro, editors, *Computer Security*, pages 107–122, Cham, 2020. Springer International Publishing.

- [10] MingJian Tang, Mamoun Alazab, and Yuxiu Luo. Big data for cybersecurity: Vulnerability disclosure trends and dependencies. *IEEE Transactions on Big Data*, 5(3):317–329, 2017.
- [11] IBM. X-force threat intelligence index 2024. last accessed: 15 June 2024.
- [12] Barnaby Stewart, Luis Rosa, Leandros A Maglaras, Tiago J Cruz, Mohamed Amine Ferrag, Paulo Simoes, and Helge Janicke. A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 4(10), 2017.
- [13] Bil Hallaq, Andrew Nicholson, Richard Smith, Leandros Maglaras, Helge Janicke, and Kevin Jones. Cyran: a hybrid cyber range for testing security on ics/scada systems. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pages 622–637. IGI Global, 2018.
- [14] Dustin Updyke, Geoffrey Dobson, Thomas Podnar, Luke Osterritter, Benjamin Earl, and Adam Cerini. Ghosts in the machine: A framework for cyber-warfare exercise npc simulation. Technical Report CMU/SEI-2018-TR-005, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2018.
- [15] UNIWA. Uniwa ctf. (last accessed: 17.01.2021).
- [16] Jon Davis and Shane Magrath. A survey of cyber ranges and testbeds executive. 2013.
- [17] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. A survey of industrial control system testbeds. In Sonja Buchegger and Mads Dam, editors, *Secure IT Systems*, pages 11–26, Cham, 2015. Springer International Publishing.
- [18] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636, 2020.
- [19] Stela Kucek and Maria Leitner. An empirical survey of functions and configurations of open-source capture the flag (ctf) environments. *Journal of Network and Computer Applications*, 151:102470, 2020.
- [20] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. A review of cyber-ranges and test-beds: current and future trends. *Sensors*, 20(24):7148, 2020.
- [21] Nestoras Chouliaras, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. A novel autonomous container-based platform for cybersecurity training and research. *PeerJ Computer Science*, 9:e1574, 2023.
- [22] David Kushner. The real story of stuxnet. *ieee Spectrum*, 50(3):48–53, 2013.
- [23] Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56, 2018.

- [24] M. Dark. Thinking about cybersecurity. *IEEE Security Privacy*, 13(1):61–65, 2015.
- [25] NIST. Cyber ranges.
- [26] Chiara Braghin, Stelvio Cimato, Ernesto Damiani, Fulvio Frati, Elvinia Riccobene, and Sadegh Astaneh. Towards the monitoring and evaluation of trainees’ activities in cyber ranges. In *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity*, pages 79–91. Springer, 2020.
- [27] Zdenek Eichler. Cloud-based security research testbed: A ddos use case.
- [28] Rik Goldman. *Learning Proxmox VE*. Packt Publishing Ltd, 2016.
- [29] Grethe Østby, Lars Berg, Mazaher Kianpour, Basel Katt, and Stewart James Kowalski. A socio-technical framework to improve cyber security training: A work in progress. CEUR Workshop Proceedings, 2019.
- [30] Elaine M Raybourn, Michael Kunz, David Fritz, and Vince Urias. A zero-entry cyber range environment for future learning ecosystems. In *Cyber-Physical Systems Security*, pages 93–109. Springer, 2018.
- [31] Cuong Pham, Dat Tang, Ken-ichi Chinen, and Razvan Beuran. Cyris: A cyber range instantiation system for facilitating security training. In *Proceedings of the Seventh Symposium on Information and Communication Technology*, pages 251–258, 2016.
- [32] E. Luchian, C. Filip, A. B. Rus, I. Ivanciu, and V. Dobrota. Automation of the infrastructure and services for an openstack deployment using chef tool. In *2016 15th RoEduNet Conference: Networking in Education and Research*, pages 1–5, 2016.
- [33] RO Kostromin. Survey of software configuration management tools of nodes in heterogeneous distributed computing environment.
- [34] Roman-Valentyn Tkachuk, Dragos Ilie, and Kurt Tutschku. Orchestrating future service chains in the next generation of clouds. In *SNCNW 2019*, pages 18–22, 2019.
- [35] Yevgeniy Brikman. Why we use terraform and not chef, puppet, ansible, saltstack, or cloudformation, 2016.
- [36] Piret Pernik. Improving cyber security: Nato and the eu. *Tallinn: International Center for Defence Studies*, 2014.
- [37] Jan Vykopal, Radek Ošlejšek, Pavel Čeleda, Martin Vizvary, and Daniel Tovarňák. Kypa cyber range: Design and use cases. 2017.
- [38] J. Vykopal, M. Vizvary, R. Oslejsek, P. Celeda, and D. Tovarnak. Lessons learned from complex hands-on defence exercises in a cyber range. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–8, 2017.
- [39] Florida Cyber Range. Florida cyber range. last accessed: 24 November 2020.
- [40] Virginia Cyber Range. About the virginia cyber range. last accessed: 25 November 2020.

- [41] Omar Darwish, Christopher M Stone, Ola Karajeh, and Belal Alsinglawi. Survey of educational cyber ranges. In *Workshops of the International Conference on Advanced Information Networking and Applications*, pages 1037–1045. Springer, 2020.
- [42] T. Debatty and W. Mees. Building a Cyber Range for Training CyberDefense Situation Awareness. In *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, pages 1–6, 2019.
- [43] S. Llopis, J. Hingant, I. Pérez, M. Esteve, F. Carvajal, W. Mees, and T. Debatty. A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, pages 1–7, May 2018.
- [44] Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, Oliver Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, and Manuel Warum. Ait cyber range: Flexible cyber security environment for exercises, training and research. In *European Interdisciplinary Cybersecurity Conference (EICC)*, pages 18–19, 2020.
- [45] M. Frank, M. Leitner, and T. Pahi. Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, pages 38–46, Nov 2017.
- [46] Stela Kucek and Maria Leitner. Training the human-in-the-loop in industrial cyber ranges. In Sophia Keil, Rainer Lasch, Fabian Lindner, and Jacob Lohmer, editors, *Digital Transformation in Semiconductor Manufacturing*, pages 107–118, Cham, 2020. Springer International Publishing.
- [47] Cynthia E. Irvine, Michael F. Thompson, Michael McCarrin, and Jean Khosalim. Live lesson: Labtainers: A docker-based framework for cybersecurity labs. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, August 2017. USENIX Association.
- [48] M. F. Thompson and C. E. Irvine. Individualizing cybersecurity lab exercises with labtainers. *IEEE Security Privacy*, 16(2):91–95, March 2018.
- [49] Grethe Østby, Lars Berg, Mazaher Kianpour, Basel Katt, and Stewart Kowalski. A socio-technical framework to improve cyber security training: A work in progress. In *STPIS@ECIS*, 2019.
- [50] M. Kianpour, S. Kowalski, E. Zoto, C. Frantz, and H. Øverby. Designing serious games for cyber ranges: A socio-technical approach. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 85–93, June 2019.
- [51] Tero Kokkonen, Timo Hämäläinen, Marko Silokunnas, Jarmo Siltanen, Mikhail Zolotukhin, and Mikko Neijonen. Analysis of approaches to internet traffic generation for cyber security research and exercise. In Sergey Balandin, Sergey Andreev, and Yevgeni Koucheryavy, editors, *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pages 254–267, Cham, 2015. Springer International Publishing.

- [52] M. Karjalainen, T. Kokkonen, and S. Puuska. Pedagogical aspects of cyber security exercises. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 103–108, June 2019.
- [53] Tommy Gustafsson and Jonas Almroth. Cyber range automation overview with a case study of crate.
- [54] H. Holm and T. Sommestad. Sved: Scanning, vulnerabilities, exploits and detection. In *MILCOM 2016 - 2016 IEEE Military Communications Conference*, pages 976–981, 2016.
- [55] Aunshul Rege, Joe Adams, Edward Parker, Brian Singer, Nicholas Masceri, and Rohan Pandit. Using cybersecurity exercises to study adversarial intrusion chains, decision-making, and group dynamics. In *European Conference on Cyber Warfare and Security*, pages 351–360. Academic Conferences International Limited, 2017.
- [56] silensec. silensec. last accessed: 24 November 2020.
- [57] Kazuhiro Hara. Cyber range cyberium for training security meisters to deal with cyber attacks. *FUJITSU SCIENTIFIC & TECHNICAL JOURNAL*, 55(5):59–63, 2019.
- [58] nuari. nuari. last accessed: 24 November 2020.
- [59] Georgia Cyber Center. Georgia cyber center. last accessed: 24 November 2020.
- [60] IBM. Ibm xforce. last accessed: 25 November 2020.
- [61] cybexer. cybexer. last accessed: 25 November 2020.
- [62] airbus. airbus cyber ranger. last accessed: 25 November 2020.
- [63] Raytheon. Raytheon cyber ranger. last accessed: 25 November 2020.
- [64] DIATEAM. hns-platform cyber ranger. last accessed: 25 November 2020.
- [65] cyberbit. cyberbit cyber range. last accessed: 25 November 2020.
- [66] Cyber Warfare Range. Cyber warfare range. last accessed: 25 November 2020.
- [67] Nestoras Chouliaras. Cyber range questionnaire. last accessed: 15 September 2020.
- [68] E. Seker and H. H. Ozbenli. The concept of cyber defence exercises (cdx): Planning, execution, evaluation. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–9, 2018.
- [69] Carlos Arturo Martinez Forero. *Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development*. PhD thesis, Master’s Thesis, 2016.
- [70] Jason Kick. Cyber exercise playbook. Technical report, MITRE CORP BEDFORD MA, 2014.

- [71] Robert Beveridge. Effectiveness of increasing realism into cybersecurity training. *International Journal of Cyber Research and Education (IJCRE)*, 2:40–54, 2020.
- [72] JYVSECTEC Jyväskylä Security Technology. Rgce organizational environments. last accessed: 25 November 2020.
- [73] Norges teknisk-naturvitenskapelige universitet. Om norwegian cyber range. last accessed: 25 November 2020.
- [74] Masaryk University. Kypo cyber range platform. last accessed: 25 November 2020.
- [75] Lucas Nussbaum. Testbeds support for reproducible research. In *Proceedings of the reproducibility workshop*, pages 24–26, 2017.
- [76] Timothy M Braje. Advanced tools for cyber ranges. Technical report, MIT Lincoln Laboratory Lexington United States, 2016.
- [77] European Cyber Security Organisation (ECSSO). Understanding cyber ranges: From hype to reality. last accessed: 25 November 2020.
- [78] Enrico Russo, Gabriele Costa, and Alessandro Armando. Building next generation cyber ranges with crack. *Computers & Security*, page 101837, 2020.
- [79] Sunny Behal and Krishan Kumar. Characterization and comparison of ddos attack tools and traffic generators: A review. *IJ Network Security*, 19(3):383–393, 2017.
- [80] B. R. Patil, M. Moharir, P. K. Mohanty, G. Shobha, and S. Sajeew. Ostinato - a powerful traffic generator. In *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, pages 1–5, 2017.
- [81] Alessio Botta, Alberto Dainotti, and Antonio Pescapè. A tool for the generation of realistic network workload for emerging networking scenarios. *Computer Networks*, 56(15):3531–3547, 2012.
- [82] Felix Erlacher and Falko Dressler. How to test an ids? genesids: An automated system for generating attack traffic. In *Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity*, pages 46–51, 2018.
- [83] Vincent H. Berk, Ian Gregorio de Souza, and John P. Murphy. Generating realistic environments for cyber operations development, testing, and training. In Edward M. Carapezza, editor, *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI*, volume 8359, pages 51 – 59. International Society for Optics and Photonics, SPIE, 2012.
- [84] Andy Applebaum, Doug Miller, Blake Strom, Chris Korban, and Ross Wolf. Intelligent, automated red team emulation. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 363–373, 2016.
- [85] Tero Kokkonen and Samir Puuska. Blue team communication and reporting for enhancing situational awareness from white team perspective in cyber security exercises. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pages 277–288. Springer, 2018.

- [86] NCCDC. National ccdc. collegiate cyber defense competition. last accessed: 25 September 2020.
- [87] Mark Evans, Ying He, Leandros Maglaras, and Helge Janicke. Heart-is: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 80:74–89, 2019.
- [88] Dimitrios Kosmanos, Nikolas Prodromou, Antonios Argyriou, Leandros A Maglaras, and Helge Janicke. Mimo techniques for jamming threat suppression in vehicular networks. *Mobile Information Systems*, 2016, 2016.
- [89] Mohamed Amine Ferrag, Leandros Maglaras, Ahmed Ahmim, Makhlof Derdour, and Helge Janicke. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future internet*, 12(3):44, 2020.
- [90] Harry Doubleday, Leandros Maglaras, and Helge Janicke. Ssh honeypot: building, deploying and analysis. 2016.
- [91] Vassilis Papaspirou, Leandros Maglaras, Mohamed Amine Ferrag, Ioanna Kantzavelou, Helge Janicke, and Theodoros Tsiftsis. A novel two-factor honeypot authentication mechanism. *arXiv preprint arXiv:2012.08782*, 2020.
- [92] Ahmad Zia Sharifi, Vajirasak Vanijja, Debajyoti Pal, and Watcharee Anantasabkit. Cyberiot: An initial conceptualization of a web-based cyber range for iot. In *2021 International Conference on Computational Performance Evaluation (ComPE)*, pages 091–096. IEEE, 2021.
- [93] Xuan Low, DeQuan Yang, and DengPan Yang. Design and implementation of industrial control cyber range system. In *2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 166–170. IEEE, 2022.
- [94] Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11(4):1809, 2021.
- [95] NIST. Cyber Ranges. <https://www.nist.gov/document/cyber-range-guide>, 2018. (accessed: 29.01.2023).
- [96] Razvan Beuran, Dat Tang, Zheyu Tan, Shinobu Hasegawa, Yasuo Tan, and Yoichi Shinoda. Supporting cybersecurity education and training via lms integration: Cylms. *Education and Information Technologies*, 24:3619–3643, 2019.
- [97] University of West Attica. The Cybersecurity Team of UNIWA in the 3rd place of the World Competition. <https://dialogoi.uniwa.gr/university/h-omada-kyvernoasfaleias-toy-pada-stin-3i-thesi-pagkosmioy-diagonismoy/>, 2022. (last accessed: 22.12.2022).
- [98] Ioanna Kantzavelou, Leandros Maglaras, Panagiotis Tzikopoulos, and Sokratis Katsikas. A Multiplayer Game Model to Detect Insiders in Wireless Sensor Networks. *PeerJ Computer Science*, 8(e791), 2022.

- [99] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 20(24):7148, 2020.
- [100] Lei Chen, Ming Xian, and Jian Liu. Monitoring system of openstack cloud platform based on prometheus. In *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, pages 206–209. IEEE, 2020.
- [101] Inc Gartner. Cool vendors in container management.
- [102] Wen-Chung Shih, Chao-Tung Yang, Rajiv Ranjan, and Chun-I Chiang. Implementation and Evaluation of a Container Management Platform on Docker: Hadoop Deployment as an Example. *Cluster Computing*, 24(4):3421–3430, 2021.
- [103] Bishwajeet Pandey and Shabeer Ahmad. *Introduction to the Cyber Ranges*. Chapman and Hall/CRC, 2022.
- [104] Toomas Lepik. Hypervisor agnostic scenario definition language for cyber ranges.
- [105] Vasyi Oleksiuk and Olesia Oleksiuk. The practice of developing the academic cloud using the proxmox ve platform. *Educational Technology Quarterly*, 2021(4):605–616, 2021.
- [106] Razvan Beuran, Zhe Zhang, and Yasuo Tan. Aws ec2 public cloud cyber range deployment. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 433–441. IEEE, 2022.
- [107] Brian Kocoloski, Alefiya Hussain, Matthew Troglia, Calvin Ardi, Steven Cheng, Dave DeAngelis, Christopher Symonds, Michael Collins, Ryan Goodfellow, and Stephen Schwab. Case studies in experiment design on a minimega based network emulation testbed. In *Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, pages 83–90, 2021.
- [108] Ryotaro Nakata and Akira Otsuka. Cyexec*: A high-performance container-based cyber range with scenario randomization. *IEEE Access*, 9:109095–109114, 2021.
- [109] Ming Mao and Marty Humphrey. A performance study on the vm startup time in the cloud. In *2012 IEEE Fifth International Conference on Cloud Computing*, pages 423–430, 2012.
- [110] Ashish Lingayat, Ranjana R Badre, and Anil Kumar Gupta. Performance Evaluation for Deploying Docker Containers on Baremetal and Virtual Machine. In *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, pages 1019–1023. IEEE, 2018.
- [111] RR Yadav, ETG Sousa, and GRA Callou. Performance Comparison between Virtual Machines and Docker Containers. *IEEE Latin America Transactions*, 16(8):2282–2288, 2018.
- [112] Inc Docker. Docker. *linea*].[Junio de 2017]. Disponible en: <https://www.docker.com/what-docker>, 2020.

- [113] Amit M Potdar, DG Narayan, Shivaraj Kengond, and Mohammed Moin Mulla. Performance evaluation of docker container and virtual machine. *Procedia Computer Science*, 171:1419–1428, 2020.
- [114] Openstack. Tools and packaging recipes to help install and maintain the lifecycle of openstack deployments., 2023. (accessed: 29.06.2023).
- [115] Haotian Zhao and Yuchen Sun. A low-ops iaas cloud framework based on cloud-native architecture. In *Proceedings of the 2024 7th International Conference on Software Engineering and Information Management*, pages 29–34, 2024.
- [116] Steffen Thielemans, Ruben De Smet, Priscilla Benedetti, Gianluca Reali, An Braeken, and Kris Steenhaut. Experiences with on-premise open source cloud infrastructure with network performance validation. In *IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society*, pages 1–6. IEEE, 2022.
- [117] Sijie Yang, Xiaofeng Wang, Xiaoxue Wang, Lun An, and Guizhu Zhang. High-performance docker integration scheme based on openstack. *World Wide Web*, 23(4):2593–2632, 2020.
- [118] Youngki Park, Hyunsik Yang, and Younghan Kim. Performance analysis of cni (container networking interface) based container network. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 248–250. IEEE, 2018.
- [119] Zakaria Benomar, Francesco Longo, Giovanni Merlino, and Antonio Puliafito. Enabling container-based fog computing with openstack. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1049–1056. IEEE, 2019.
- [120] Martin Macak, Radek Oslejsek, and Barbora Buhnova. Process mining analysis of puzzle-based cybersecurity training. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, pages 449–455, 2022.
- [121] Leandros Maglaras and Ioanna Kantzavelou, editors. *Cybersecurity Issues in Emerging Technologies*. CRC Press, 2021.
- [122] NHS Simanullang and J Rajagukguk. Learning management system (lms) based on moodle to improve students learning activity. In *Journal of Physics: Conference Series*, volume 1462, page 012067. IOP Publishing, 2020.
- [123] Darren Turnbull, Ritesh Chugh, and Jo Luck. Learning management systems, an overview. *Encyclopedia of education and information technologies*, pages 1052–1058, 2020.
- [124] Brian Brazil. *Prometheus: Up & Running: Infrastructure and Application Performance Monitoring*. " O'Reilly Media, Inc.", 2018.

- [125] Jan Vykopal, Pavel Čeleda, Pavel Seda, Valdemar Švábenský, and Daniel Tovarňák. Scalable Learning Environments for Teaching Cybersecurity Hands-on. In *2021 IEEE Frontiers in Education Conference (FIE)*, pages 1–9, 2021.
- [126] Openstack. Openstack. <https://www.openstack.org/>, 2023. (accessed: 29.01.2023).
- [127] Michael Thompson and Cynthia Irvine. Labtainers Cyber Exercises: Building and Deploying Fully Provisioned Cyber Labs that Run on a Laptop. In *SIGCSE*, page 1353, 2021.
- [128] Ryotaro Nakata and Akira Otsuka. Cyexec*: A High-Performance Container-based Cyber Range with Scenario Randomization. *IEEE Access*, 9:109095–109114, 2021.
- [129] Sanggyu Shin, Yoichi Seto, Yosuke Kasai, Rituna Ka, Daishi Kuroki, Shinichi Toyoda, Koji Hasegawa, and Kazuhiro Midorikawa. Development of Training System and Practice Contents for Cybersecurity Education. In *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, pages 172–177, 2019.
- [130] Ansible. Red Hat, Inc. Red Hat Ansible Automation Platform. <https://www.ansible.com/>, 2020. (last accessed: 06.12.2022).
- [131] Tomas Lieskovan and Jan Hajný. Building open source cyber range to teach cyber security. In *Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES 21, New York, NY, USA, 2021*. Association for Computing Machinery.
- [132] Borka Jerman Blažič. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, 27(3):3011–3036, 2022.
- [133] Forbes.com. How Tech Companies Can Help Solve the Cybersecurity Skills Shortage. <https://www.forbes.com/sites/forbestechcouncil/2021/11/23/how-tech-companies-can-help-solve-the-cybersecurity-skills-shortage/>, 2022. (last accessed: 06.05.2022).
- [134] Ioanna Kantzavelou, Panagiotis F. Tzikopoulos, and Sokratis K. Katsikas. Detecting Intrusive Activities from Insiders in a Wireless Sensor Network Using Game Theory. In *Proceedings of the 6th International Conference on Pervasive Technologies Related to Assistive Environments, PETRA '13, New York, NY, USA, 2013*. Association for Computing Machinery.
- [135] Inc Gartner. Predicts 2023: Cybersecurity industry focuses on the human deal.
- [136] Yagmur Yigit, Kitty Kioskli, Laura Bishop, Nestoras Chouliaras, Leandros Maglaras, and Helge Janicke. Enhancing cybersecurity training efficacy: A comprehensive analysis of gamified learning, behavioral strategies and digital twins. In *2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 24–32, 2024.
- [137] Cheryl Beauchamp and Holly Matusovich. A mixed-method study exploring cyber ranges and educator motivation. *Journal of Cybersecurity Education Research and Practice*, 2023.

- [138] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009.
- [139] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77:226–261, 2018.
- [140] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke. From game design elements to gamefulness: defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, page 9–15, New York, NY, USA, 2011. Association for Computing Machinery.
- [141] Xiao, Hanyu, Wei, Hao, Liao, Qichen, Ye, Qiongwei, Cao, Changlin, and Zhong, Yawen. Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. *SHS Web of Conf.*, 166:01036, 2023.
- [142] Michael Grieves. Digital twin: manufacturing excellence through virtual factory replication. *White paper*, 1(2014):1–7, 2014.
- [143] Rossouw von Solms and Johan van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, 2013. Cybercrime in the Digital Economy.
- [144] Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3:1–18, 2020.
- [145]Carolynn P Scherer and Christy E Ruggiero. Overview of tools for insider threat: Analysis and mitigation. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2019.
- [146] Leandros A Maglaras and Jianmin Jiang. A real time ocsvm intrusion detection module with low overhead for scada systems. *International Journal of Advanced Research in Artificial Intelligence (IJARAI)*, 3(10), 2014.
- [147] Georgeta Catescu. *Detecting insider threats using Security Information and Event Management (SIEM)*. PhD thesis, UAS Technikum Wien, 2018.
- [148] David S Wall. Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, 26(2):107–124, 2013.
- [149] Nebrase Elmrabbit, Shuang-Hua Yang, and Lili Yang. Insider threats in information security categories and approaches. In *2015 21st International Conference on Automation and Computing (ICAC)*, pages 1–6. IEEE, 2015.
- [150] Cost of insider threats global report: Proofpoint us, Jun 2020.
- [151] B Obama. National insider threat policy and minimum standards for executive branch insider threat programs. *Office of the Press Secretary*, page 1, 2012.

- [152] Nebrase Elmrbait. *A multiple-perspective approach for insider-threat risk prediction in cyber-security*. PhD thesis, Loughborough University, 2018.
- [153] Imelda Zadeja and Jozef Bushati. Gamification and serious games methodologies in education. In *International Symposium on Graphic Engineering and Design*, pages 599–605, 2022.
- [154] Tommy van Steen and Julia RA Deeleman. Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9):593–598, 2021.
- [155] Richard M Ryan and Edward L Deci. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, 55(1):68, 2000.
- [156] Edward L Deci, Anja H Olafsen, and Richard M Ryan. Self-determination theory in work organizations: The state of a science. *Annual review of organizational psychology and organizational behavior*, 4:19–43, 2017.
- [157] Frédéric Guay, Robert J Vallerand, and Céline Blanchard. On the assessment of situational intrinsic and extrinsic motivation: The situational motivation scale (sims). *Motivation and emotion*, 24:175–213, 2000.
- [158] USwitch. Online Gaming Statistics 2023 kernel description, 2023.
- [159] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 915–928, 2013.
- [160] Srishti Kulshrestha, Sarthak Agrawal, Devottam Gaurav, Manmohan Chaturvedi, Subodh Sharma, and Ranjan Bose. Development and validation of serious games for teaching cybersecurity. In *Serious Games: Joint International Conference, JCSG 2021, Virtual Event, January 12–13, 2022, Proceedings 7*, pages 247–262. Springer, 2021.
- [161] Mikel Salazar, José Gaviria, Carlos Laorden, and Pablo G Bringas. Enhancing cybersecurity learning through an augmented reality-based serious game. In *2013 IEEE global engineering education conference (EDUCON)*, pages 602–607. IEEE, 2013.
- [162] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95:101827, 2020.
- [163] Sam Scholefield and Lynsay A Shepherd. Gamification techniques for raising cyber security awareness. In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, pages 191–203. Springer, 2019.

- [164] Mónica Stambuk Castellano, Ignacio Contreras-McKay, Andrés Neyem, Emilio Farfán, Oscar Inzunza, Nicolás E Ottone, Mariano Del Sol, Carlos Alario-Hoyos, Macarena Soto Alvarado, and R Shane Tubbs. Empowering human anatomy education through gamification and artificial intelligence: An innovative approach to knowledge appropriation. *Clinical Anatomy*, 37(1):12–24, 2024.
- [165] Liuyufeng Li, Khe Foon Hew, and Jiahui Du. Gamification enhances student intrinsic motivation, perceptions of autonomy and relatedness, but minimal impact on competency: a meta-analysis and systematic review. *Educational technology research and development*, pages 1–32, 2024.
- [166] JM Blythe. Using behavioural insights to improve the public’s use of cyber security best practices. *Government office for science*, 2014.
- [167] Magdalena Glas, Fabian Böhm, Falko Schönteich, and Günther Pernul. Cyber range exercises: Potentials and open challenges for organizations. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 24–35. Springer, 2023.
- [168] Jose Gomez, Elie F Kfoury, Jorge Crichigno, and Gautam Srivastava. A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, 237:110054, 2023.
- [169] Borka Jerman Blažič. The cybersecurity labour shortage in europe: Moving to a new concept for education and training. *Technology in Society*, 67:101769, 2021.
- [170] Jan Hajny, Marek Sikora, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. Adding european cybersecurity skills framework into curricula designer. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–6, 2022.
- [171] ENISA. European Cybersecurity Skills Framework (ECSF). <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>, 2023. (last accessed: 22.12.2023).
- [172] ISACs EU. Information Sharing and Analysis Centres EU. <https://www.isacs.eu/>, 2022. (last accessed: 22.12.2022).
- [173] Jan Vykopal, Pavel Seda, Valdemar Švábenskỳ, and Pavel Čeleda. Smart environment for adaptive learning of cybersecurity skills. *IEEE Transactions on Learning Technologies*, 2022.
- [174] Fraser Hall, Leandros Maglaras, Theodoros Aivaliotis, Loukas Xagoraris, and Ioanna Kantzavelou. Smart Homes: Security Challenges and Privacy Concerns. *arXiv preprint arXiv:2010.15394v1 [cs.CR]*, 2020.
- [175] Ellak. Call for Participation in Panoptis 2022 Cyber Defence Exercise, <https://privacy.ellak.gr/2022/05/13/kalesma-gia-simmetochi-se-omada-gia-tin-askisi-kivernoaminas-panoptis-2022/>, 2022. (last accessed: 22.12.2022).
- [176] ITU. Cyberdrills. <https://www.itu.int/en/itu-d/cybersecurity/pages/cyberdrills.aspx>, 2022. (last accessed: 29.01.2023).

- [177] Stylianos Karagiannis and Emmanouil Magkos. Adapting CTF Challenges into Virtual Cybersecurity Learning Environments. *Information & Computer Security*, 29(1):105–132, 2020.
- [178] Gideon N Angafor, Iryna Yevseyeva, and Ying He. Game-based Learning: A Review of Tabletop Exercises for Cybersecurity Incident Response Training. *Security and Privacy*, 3(6):e126, 2020.
- [179] Allan Cook, Richard G Smith, Leandros Maglaras, and Helge Janicke. Scips: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control System. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 7(2):1–15, 2017.
- [180] Stylianos Karagiannis, Christoforos Ntantogian, Emmanouil Magkos, Luís L. Ribeiro, and Luís Campos. PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. *Information*, 12(8), 2021.
- [181] Chris Eagle. Computer Security Competitions: Expanding Educational Outcomes. *IEEE Security & Privacy*, 11(4):69–71, 2013.
- [182] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.
- [183] NARUC. Cybersecurity Tabletop Exercise Guide, 2021. (last accessed: 22.12.2023).
- [184] Gideon N Angafor, Iryna Yevseyeva, and Ying He. Bridging the cyber security skills gap: Using tabletop exercises to solve the cssg crisis. In *Joint International Conference on Serious Games*, pages 117–131. Springer, 2020.
- [185] NIST CVE-2020-28036. wp-includes/class-wp-xmlrpc-server.php in WordPress before 5.5.2 allows attackers to gain privileges by using XML-RPC to comment on a post <https://nvd.nist.gov/vuln/detail/cve-2020-28036>, 2020. (last accessed: 06.05.2022).
- [186] Robin Wood. Damn vulnerable web application (dvwa). URL: <https://github.com/digininja/DVWA> (visited on 02/15/2021), 2022.
- [187] Νέστορας Χουλιάρας. Empirical evaluation of state-of-the-art penetration tools. 2017.

Appendix A

Publications

The ideas presented in this thesis appear in the following publications:

Journal articles / Book chapters / Conference proceedings

1. Nestoras Chouliaras, Leandros Maglaras, Ioanna Kantzavelou, Grammati Pantziou, Panagiota Chouliara-Sidera, Antonia Adamakos, Panagiotis Chalatsakos, ETHACA - A container-based cyber range for research and education, IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2024), 21-23 October 2024, Athens, Greece
2. Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11(4):1809, 2021.
3. Chouliaras, N.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. A novel autonomous container-based platform for cybersecurity training and research. *PeerJ Comput. Sci.* 2023, 9, e1574.
4. Yagmur Yigit, Kitty Kioskli, Laura Bishop, Nestoras Chouliaras, Leandros Maglaras, Helge Janicke, "Enhancing Cybersecurity Training Efficacy: A Comprehensive Anal-

ysis of Gamified Learning, Behavioral Strategies and Digital Twins" 25th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM 2024), June 04-07 2024, Perth, Australia

5. Dimitrios Tsiostas, George Kittes, Nestoras Chouliaras, Ioanna Kantzavelou, Leandros Maglaras, Christos Douligeris and Vasileios Vlachos, "The Insider Threat: Reasons, Effects and Mitigation Techniques", 24th Pan-Hellenic Conference on Informatics (PCI 2020), Athens, Greece, November 20th-22nd, 2020, DOI: 10.1145/3437120.3437336.

Other publications:

Journal articles / Book chapters / Conference proceedings

1. Leandros Maglaras, George Drivas, Nestoras Chouliaras, Eerke Boiten, Costas Lambri-noudakis, and Sotiris Ioannidis. Cybersecurity in the era of digital transformation: the case of greece. In 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), pages 1–5. IEEE, 2020.
2. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electron. Electr. Eng.* 2021, 5, 24–37.
3. Tsiostas, D.; Kittes, G.; Chouliaras, N.; Kantzavelou, I.; Maglaras, L.; Douligeris, C.; Vlachos, V. The Insider Threat: Reasons, Effects and Mitigation Techniques. In *Proceedings of the 24th Pan-Hellenic Conference on Informatics, Athens, Greece, 20–22 November 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 340–345
4. P. Efstathiadis, A. Karanika, N. Chouliaras, L. Maglaras and I. Kantzavelou, "Smart cars and over-the-air updates" in *Cybersecurity Issues in Emerging Technologies*, Boca Raton, FL, USA:CRC Press, 2021.
5. Clark, N., Maglaras, L., Kantzavelou, I., Chouliaras, N., Ferrag, M.A.: Blockchain technology: security and privacy issues. In: Patnaik, S., Wang, T.-S., Shen, T.,

Panigrahi, S.K. (eds.) Blockchain Technology and Innovations in Business Processes. SIST, vol. 219, pp. 95–107. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-6470-7_6

Appendix B

Εκτεταμένη Περίληψη στα Ελληνικά

Το παράρτημα αυτό περιλαμβάνει μία εκτεταμένη περίληψη της διατριβής στην ελληνική γλώσσα. Κάθε ενότητα της εκτεταμένης περίληψης αφορά ένα κεφάλαιο του αγγλικού κειμένου.

Κεφάλαιο 1

Στην ψηφιακή εποχή, η δομή της παγκόσμιας κοινωνίας μας διαμορφώνεται ολοένα και περισσότερο από την τεχνολογία, καθιστώντας την κυβερνοασφάλεια όχι απλώς ένα ζήτημα προστασίας των πληροφοριών, αλλά μια θεμελιώδη βάση της εθνικής και διεθνούς ασφάλειας. Η αυξανόμενη εξάρτησή μας από την τεχνολογία απαιτεί έναν αναβαθμισμένο τρόπο σκέψης σχετικά με την ασφάλεια, ο οποίος να περιλαμβάνει τόσο την προστασία δεδομένων όσο και τη θωράκιση των κρίσιμων υποδομών που διασφαλίζουν την ευημερία των κοινωνιών μας. Η συχνότητα και ο αντίκτυπος των κυβερνοεπιθέσεων έχουν αυξηθεί δραματικά, στοχεύοντας ζωτικές υποδομές, εταιρείες, ακόμη και έθνη, με συνέπειες που διαπερνούν όλες τις πτυχές της κοινωνίας. Αυτή η κλιμάκωση υπογραμμίζει την κρίσιμη, επείγουσα ανάγκη για ισχυρή εκπαίδευση και έρευνα στην κυβερνοασφάλεια. Η ανάπτυξη αποτελεσματικών στρατηγικών για την αντιμετώπιση των κυβερνοαπειλών και τη διασφάλιση της ανθεκτικότητας των ψηφιακών μας υποδομών είναι υψίστης σημασίας.

Σε αυτό το πλαίσιο, τα συστήματα **Cyber Range** αναδεικνύονται ως απαραίτητα εργαλεία για την εκπαίδευση και την έρευνα στην κυβερνοασφάλεια.

Τα **Cyber Range** είναι περιβάλλοντα εξελιγμένα, προσομοιωμένα και σχεδιασμένα να αντικατοπτρίζουν την πολύπλοκη φύση των πραγματικών υποδομών πληροφορικής και δικτύων, παρέχοντας έναν ασφαλή χώρο όπου οι κυβερνοαπειλές μπορούν να προσομοιωθούν, μελετηθούν και αντιμετωπιστούν. Αυτές οι σύγχρονες πλατφόρμες διευκολύνουν μια πρακτική προσέγγιση στην κυβερνοασφάλεια, επιτρέποντας στους φοιτητές και στους ερευνητές να αναπτύξουν τις δεξιότητές τους, να αναπτύξουν νέα μέτρα αντιμετώπισης και να κατανοήσουν πλήρως την ανατομία των κυβερνοεπιθέσεων σε ένα ελεγχόμενο, αλλά ρεαλιστικό περιβάλλον. Προσομοιώνοντας κυβερνοεπιθέσεις, μηχανισμούς άμυνας και ακόμη και τις αλυσιδωτές επιπτώσεις των παραβιάσεων σε ψηφιακά συστήματα, τα συστήματα **Cyber Range** διαδραματίζουν καθοριστικό ρόλο στην προετοιμασία της επόμενης γενιάς επαγγελματιών κυβερνοασφάλειας και στην προώθηση της έρευνας στον τομέα της κυβερνοασφάλειας. Οι παραδοσιακές προσεγγίσεις βασίζονται συχνά σε θεωρητικές γνώσεις, προσφέροντας περιορισμένες ευκαιρίες για πρακτική εφαρμογή. Αντίθετα, τα συστήματα **Cyber Range** επιτρέπουν μια δυναμική, διαδραστική εμπειρία μάθησης που γεφυρώνει το χάσμα μεταξύ θεωρίας και πράξης.

Καθώς οι κυβερνοαπειλές συνεχίζουν να εξελίσσονται σε πολυπλοκότητα και έκταση, η σημασία των συστημάτων **Cyber Range** στην ανάπτυξη αποτελεσματικών στρατηγικών κυβερνοασφάλειας γίνεται όλο και πιο εμφανής. Αυτά τα συστήματα όχι μόνο εξοπλίζουν τους φοιτητές με τις απαραίτητες δεξιότητες και γνώσεις για να προστατεύσουν τα ψηφιακά περιουσιακά στοιχεία, αλλά παρέχουν επίσης στους ερευνητές ένα ευέλικτο εργαλείο για την εξερεύνηση καινοτόμων λύσεων στην κυβερνοασφάλεια. Με αυτή την έννοια, η διερεύνηση των συστημάτων **Cyber Range** στους τομείς της εκπαίδευσης και της έρευνας είναι όχι μόνο επίκαιρη αλλά και απαραίτητη, σηματοδοτώντας μια νέα εποχή στην καταπολέμηση των κυβερνοαπειλών.

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις, ειδικά αυτές που στοχεύουν συστήματα που διατηρούν ή επεξεργάζονται ευαίσθητες πληροφορίες, γίνονται πιο εξελιγμένες. Οι κρίσιμες εθνικές υποδομές είναι οι κύριοι στόχοι των κυβερνοεπιθέσεων, καθώς βασικές

πληροφορίες ή υπηρεσίες εξαρτώνται από τα συστήματά τους και η προστασία τους γίνεται σημαντικό ζήτημα που αφορά τόσο τις οργανισμούς όσο και τα έθνη. Οι επιθέσεις σε τέτοια κρίσιμα συστήματα περιλαμβάνουν διεισδύσεις στο δίκτυό τους και εγκατάσταση κακόβουλων εργαλείων ή προγραμμάτων που μπορούν να αποκαλύψουν ευαίσθητα δεδομένα ή να αλλάξουν τη συμπεριφορά συγκεκριμένου φυσικού εξοπλισμού.

Η εμφάνιση των συστημάτων **Cyber Range** σηματοδοτεί μια σημαντική εξέλιξη στον τομέα της κυβερνοασφάλειας, μεταβαίνοντας από πρωτόγονα περιβάλλοντα δοκιμής δικτύων σε εξελιγμένες πλατφόρμες που προσομοιώνουν σύνθετα κυβερνοοικοσυστήματα. Αυτή η πορεία αντανάχλα το μεταβαλλόμενη τοπίο των κυβερνοαπειλών και την αυξανόμενη ανάγκη για προηγμένους μηχανισμούς άμυνας.

Αρχικά, η έννοια του **Cyber Range** ήταν παρόμοια με τα παραδοσιακά περιβάλλοντα δοκιμής δικτύων, επικεντρωμένη κυρίως στην αξιολόγηση της αντοχής των δικτυακών αμυνών ενάντια σε ένα περιορισμένο σύνολο ευπαθειών. Αυτές οι πρώιμες εκδόσεις ήταν απαραίτητες για την κατανόηση των ευπαθειών των δικτύων και των βασικών αρχών ανίχνευσης εισβολών, αλλά δεν κατάφερναν να αποτυπώσουν την πολυδιάστατη φύση των σύγχρονων κυβερνοαπειλών. Καθώς το διαδίκτυο και οι ψηφιακές τεχνολογίες πολλαπλασιάζονταν, η πολυπλοκότητα και η εξέλιξη των κυβερνοεπιθέσεων κλιμακώνονταν, προκαλώντας μια μετατόπιση προς πιο δυναμικές και ολοκληρωμένες λύσεις εκπαίδευσης και έρευνας.

Τα σημερινά συστήματα **Cyber Range** είναι σχεδιασμένα να μιμούνται τις πραγματικές υποδομές πληροφορικής, εφαρμογές και υπηρεσίες, ενσωματώνοντας τις τελευταίες τεχνολογίες εικονικοποίησης και τεχνικές προσομοίωσης. Αυτά τα περιβάλλοντα παρέχουν ένα ρεαλιστικό υπόβαθρο ενάντια στο οποίο μπορεί να προσομοιωθεί και να αντιμετωπιστεί ένα ευρύ φάσμα κυβερνοαπειλών, από απλές εισαγωγές κακόβουλου λογισμικού έως εξελιγμένες, κρατικές κυβερνοεπιθέσεις.

Στον τομέα της εκπαίδευσης, τα συστήματα **Cyber Range** προσπαθούν να αλλάξουν τον τρόπο που διδάσκεται η κυβερνοασφάλεια. Πέρα από τη θεωρητική γνώση, προσφέρουν στους φοιτητές και τους εκπαιδευόμενους πρακτική εμπειρία στην ανίχνευση, την απόκριση και την αντιμετώπιση των κυβερνοαπειλών. Αυτή η προσέγγιση της ε-

μπειρικής μάθησης είναι ανεκτίμητη για την ανάπτυξη των πρακτικών δεξιοτήτων που απαιτούνται για να αντιμετωπίσουν τις πολυπλοκότητες του σημερινού τοπίου της κυβερνοασφάλειας. Οι εκπαιδευόμενοι δεν διδάσκονται μόνο πώς να χρησιμοποιούν εργαλεία και τεχνικές, αλλά καλούνται επίσης να σκεφτούν κριτικά, αντικατοπτρίζοντας τα πραγματικά σενάρια που θα συναντήσουν στην επαγγελματική τους ζωή.

Παρομοίως, στην έρευνα, τα συστήματα **Cyber Range** λειτουργούν ως απαραίτητα εργαλεία για τη διερεύνηση των κυβερνοαπειλών και της αποτελεσματικότητας των μηχανισμών άμυνας. Οι ερευνητές χρησιμοποιούν αυτές τις πλατφόρμες για να πραγματοποιούν ελεγχόμενα πειράματα, να δοκιμάζουν νέους μηχανισμούς άμυνας και να μελετούν τη συμπεριφορά του κακόβουλου λογισμικού σε ασφαλές περιβάλλον. Αυτή η δυνατότητα προσομοίωσης ρεαλιστικών κυβερνοεπιθέσεων και άμυνας προσφέρει κρίσιμες γνώσεις για την προώθηση του τομέα της κυβερνοασφάλειας.

Η εξέλιξη των συστημάτων **Cyber Range** από απλά περιβάλλοντα δοκιμών σε πολύπλοκους προσομοιωτές σηματοδοτεί μια κρίσιμη πρόοδο στην προσέγγισή μας στην εκπαίδευση και την έρευνα στην κυβερνοασφάλεια. Παρέχοντας μια ρεαλιστική, πρακτική εμπειρία, αυτά τα συστήματα διαδραματίζουν καθοριστικό ρόλο στην προετοιμασία της επόμενης γενιάς επαγγελματιών κυβερνοασφάλειας και στην προώθηση της κατανόησής μας για τις κυβερνοαπειλές και την άμυνα. Καθώς συνεχίζουμε να αντιμετωπίζουμε όλο και πιο εξελιγμένες κυβερνοεπιθέσεις, η σημασία των συστημάτων **Cyber Range** στην ανάπτυξη ανθεκτικών στρατηγικών κυβερνοασφάλειας δεν μπορεί να υποτιμηθεί.

Παρά τις σημαντικές προόδους στα συστήματα **Cyber Range**, παραμένουν αρκετές προκλήσεις και κενά που εμποδίζουν την πλήρη αξιοποίησή τους στην εκπαίδευση και την έρευνα στην κυβερνοασφάλεια. Τα ζητήματα αυτά αφορούν κυρίως την κλίμακωση, την προσαρμοστικότητα και την ενσωμάτωση με υπάρχοντα τεχνολογικά και εκπαιδευτικά πλαίσια, δημιουργώντας σημαντικά εμπόδια για την αποτελεσματική χρήση και την ευρεία υιοθέτηση των συστημάτων **Cyber Range**.

- Προκλήσεις Κλιμάκωσης: Καθώς οι κυβερνοαπειλές αυξάνονται σε πολυπλοκότητα και όγκο, η ανάγκη για τα συστήματα **Cyber Range** να προσομοιώνουν αυτές τις απειλές σε πραγματικό χρόνο και σε μεγάλη κλίμακα έχει γίνει επιτακτική. Τα

τρέχοντα συστήματα συχνά δυσκολεύονται να κλιμακωθούν ώστε να φιλοξενήσουν μεγάλο αριθμό χρηστών ταυτόχρονα ή να αναπαράγουν με ακρίβεια μεγάλης κλίμακας **Cyber Range**. Αυτός ο περιορισμός μειώνει την ικανότητα των εκπαιδευτικών ιδρυμάτων και των ερευνητικών οργανισμών να παρέχουν ολοκληρωμένη εκπαίδευση και να διεξάγουν εκτενή έρευνα, ιδίως όταν εξετάζουν μεγάλης κλίμακας κυβερνοπεριστατικά ή δοκιμάζουν την ανθεκτικότητα των δικτύων σε σενάρια στρες τεστ.

- **Θέματα Προσαρμοστικότητας:** Η δυναμική φύση του τοπίου της κυβερνοασφάλειας απαιτεί συστήματα **Cyber Range** που μπορούν να προσαρμοστούν γρήγορα σε αναδυόμενες απειλές και εξελισσόμενα τεχνολογικά πρότυπα. Ωστόσο, πολλά υπάρχοντα συστήματα στερούνται της ευελιξίας που χρειάζεται για την άμεση ενημέρωση ή τροποποίηση των προσομοιώσεων και των περιβαλλόντων. Αυτή η έλλειψη ευελιξίας μπορεί να οδηγήσει σε ξεπερασμένα εκπαιδευτικά προγράμματα που δεν αντικατοπτρίζουν τις τελευταίες απειλές ή τις τεχνολογικές εξελίξεις, μειώνοντας έτσι την αποτελεσματικότητα της εκπαίδευσης και της προετοιμασίας στον τομέα της κυβερνοασφάλειας.
- **Ενσωμάτωση σε Τεχνολογικά και Εκπαιδευτικά Πλαίσια:** Η αποτελεσματική ενσωμάτωση των συστημάτων **Cyber Range** στις υπάρχουσες τεχνολογικές υποδομές και τα εκπαιδευτικά προγράμματα παραμένει μια σημαντική πρόκληση. Πολλά συστήματα **Cyber Range** λειτουργούν μεμονωμένα, χωρίς απρόσκοπτη ενσωμάτωση με συστήματα διαχείρισης μάθησης, εκπαιδευτικά εργαλεία ή την ευρύτερη υποδομή πληροφορικής ενός οργανισμού. Αυτή η αποσύνδεση περιπλέκει την εμπειρία του χρήστη, περιορίζει την πρόσβαση στις λειτουργίες των **Cyber Range** και δυσχεραίνει την ικανότητα των εκπαιδευτικών να ενσωματώσουν την πρακτική εκπαίδευση στην κυβερνοασφάλεια στις διδακτικές τους μεθόδους.

Δεδομένων αυτών των προκλήσεων, υπάρχει επείγουσα ανάγκη για έρευνα και ανάπτυξη πιο ευέλικτων, κλιμακώσιμων και προσβάσιμων αρχιτεκτονικών **Cyber Range**. Τέτοιες αρχιτεκτονικές θα πρέπει να σχεδιάζονται με τη δυνατότητα προσομοίωσης μιας

ευρείας γκάμας κυβερνοαπειλών σε μεγάλη κλίμακα, επιτρέποντας τη φιλοξενία μεγάλου αριθμού ταυτόχρονων χρηστών χωρίς να υπονομεύεται η πιστότητα ή η πολυπλοκότητα της προσομοίωσης.

Επιπλέον, πρέπει να είναι προσαρμόσιμα, επιτρέποντας γρήγορες ενημερώσεις και τροποποιήσεις για να αντανακλούν τις τελευταίες κυβερνοαπειλές και τεχνολογικές εξελίξεις. Τέλος, πρέπει να δοθεί προτεραιότητα στις δυνατότητες ενσωμάτωσης, διασφαλίζοντας ότι τα συστήματα **Cyber Range** μπορούν να ενσωματωθούν απρόσκοπτα στα υπάρχοντα τεχνολογικά και εκπαιδευτικά πλαίσια, ενισχύοντας την προσβασιμότητα και τη χρησιμότητα για τους εκπαιδευτικούς και τους μαθητές.

Η αντιμετώπιση αυτών των κενών απαιτεί μια συντονισμένη προσπάθεια για καινοτομία και επανασχεδιασμό των συστημάτων **Cyber Range**. Με την ανάπτυξη αρχιτεκτονικών **Cyber Range** που είναι εναρμονισμένες με τις ανάγκες της σύγχρονης εκπαίδευσης και έρευνας στην κυβερνοασφάλεια, μπορούμε να βελτιώσουμε σημαντικά την προετοιμασία των μελλοντικών επαγγελματιών της κυβερνοασφάλειας και την αποτελεσματικότητα των στρατηγικών άμυνας στον κυβερνοχώρο.

Αυτή η διατριβή αποσκοπεί στην αντιμετώπιση των επείγουσων προκλήσεων που αντιμετωπίζουν τα τρέχοντα συστήματα **Cyber Range**, όπως προσδιορίζονται στη δήλωση προβλήματος, μέσω της ανάπτυξης μιας νέας αρχιτεκτονικής συστήματος του **ETHCA Cyber Range**. Ο πρωταρχικός στόχος είναι η ενίσχυση της κλιμάκωσης, της προσαρμοστικότητας και των δυνατοτήτων ενσωμάτωσης των συστημάτων **Cyber Range**, βελτιώνοντας έτσι σημαντικά την αποτελεσματικότητά τους στην εκπαίδευση και την έρευνα στην κυβερνοασφάλεια. Για την επίτευξη αυτού του γενικού στόχου, η έρευνα είναι δομημένη γύρω από αρκετούς συγκεκριμένους στόχους:

1. Διενέργεια Περιεκτικής Συγκριτικής Ανάλυσης των Υπαρχόντων Συστημάτων **Cyber Range**: Για να τεθούν τα θεμέλια αυτής της έρευνας, πραγματοποιήθηκε εκτενής ανασκόπηση και συγκριτική ανάλυση των τρεχόντων συστημάτων **Cyber Range**. Αυτή η ανάλυση επικεντρώθηκε στην αξιολόγηση των δυνατοτήτων κλιμάκωσης, προσαρμοστικότητας και ενσωμάτωσης των συστημάτων με τα υπάρχοντα τεχνολογικά και εκπαιδευτικά πλαίσια. Ο στόχος είναι να εντοπιστούν τα πλεονεκτήματα

και οι αδυναμίες των τρεχόντων συστημάτων, παρέχοντας κρίσιμες γνώσεις που θα ενημερώσουν τον σχεδιασμό της νέας αρχιτεκτονικής **Cyber Range**.

2. Σχεδιασμός μιας Νέας Αρχιτεκτονικής Συστήματος **Cyber Range** : Βασισμένοι στις γνώσεις που αποκτήθηκαν από τη συγκριτική ανάλυση, ο επόμενος στόχος ήταν ο σχεδιασμός μιας νέας αρχιτεκτονικής συστήματος **Cyber Range** . Η αρχιτεκτονική αντιμετωπίζει συγκεκριμένα τους προσδιορισμένους περιορισμούς, ενσωματώνοντας προηγμένα χαρακτηριστικά κλιμάκωσης, εξασφαλίζοντας ευελιξία για ενημερώσεις και τροποποιήσεις, και διευκολύνοντας την απρόσκοπτη ενσωμάτωση με εκπαιδευτικές και τεχνολογικές υποδομές. Η διαδικασία σχεδιασμού περιλαμβάνει τη διαμόρφωση λεπτομερών προδιαγραφών που ευθυγραμμίζονται με τις απαιτήσεις για αποτελεσματική εκπαίδευση και έρευνα στην κυβερνοασφάλεια.
3. Ανάπτυξη και Εφαρμογή της Προτεινόμενης Αρχιτεκτονικής Συστήματος **Cyber Range**: Αυτός ο στόχος περιλαμβάνει την τεχνική υλοποίηση του συστήματος **Cyber Range**, διασφαλίζοντας ότι ο θεωρητικός σχεδιασμός μεταφράζεται σε μια λειτουργική, κλιμακώσιμη και προσαρμοστική πλατφόρμα. Η διαδικασία ανάπτυξης έχει δώσει ιδιαίτερη προσοχή στις δυνατότητες ενσωμάτωσης, με στόχο τη δημιουργία ενός συστήματος **Cyber Range** που μπορεί να ενσωματωθεί εύκολα στα υπάρχοντα εκπαιδευτικά και τεχνολογικά περιβάλλοντα.
4. Αξιολόγηση της Αποτελεσματικότητας του Νέου Συστήματος **Cyber Range** σε Εκπαιδευτικά και Ερευνητικά Πλαίσια: Ο τελικός στόχος περιλαμβάνει μια περιεκτική αξιολόγηση της αποτελεσματικότητας του αναπτυγμένου συστήματος **Cyber Range** τόσο σε εκπαιδευτικά όσο και σε ερευνητικά περιβάλλοντα. Αυτή η αξιολόγηση θα εξετάσει τις δυνατότητες κλιμάκωσης, προσαρμοστικότητας και ενσωμάτωσης του συστήματος σε πραγματικά σενάρια, μετρώντας τον αντίκτυπό του στην ενίσχυση των αποτελεσμάτων εκπαίδευσης και έρευνας στην κυβερνοασφάλεια. Τα κριτήρια αξιολόγησης θα περιλαμβάνουν ανατροφοδότηση από τους χρήστες, μετρικές απόδοσης και την ικανότητα του συστήματος να προσομοιώνει με ακρίβεια και σε μεγάλη κλίμακα μια ευρεία γκάμα κυβερνοαπειλών.

5. Παροχή Συστάσεων για Μελλοντική Ανάπτυξη Συστημάτων **Cyber Range** : Με βάση τα ευρήματα της φάσης αξιολόγησης, η διατριβή θα ολοκληρωθεί με συστάσεις για μελλοντική ανάπτυξη και έρευνα στον τομέα των συστημάτων **Cyber Range**. Αυτές οι συστάσεις θα στοχεύουν στην καθοδήγηση συνεχών προσπαθειών για τη βελτίωση και την ενίσχυση των συστημάτων **Cyber Range** , διασφαλίζοντας ότι παραμένουν αποτελεσματικά εργαλεία για την καταπολέμηση του συνεχώς εξελισσόμενου τοπίου των κυβερνοαπειλών.

Η επίτευξη αυτών των στόχων θα συμβάλει σημαντικά στον τομέα της εκπαίδευσης και της έρευνας στην κυβερνοασφάλεια, προσφέροντας μια πιο αποτελεσματική, κλιμακώσιμη και προσαρμοστική αρχιτεκτονική συστήματος **Cyber Range** που ανταποκρίνεται καλύτερα στις ανάγκες των φοιτητών, των εκπαιδευτικών και των ερευνητών στην ψηφιακή εποχή.

Η συμβολή της διατριβής εκτείνεται από την ανασκόπηση της υπάρχουσας τεχνολογίας και την πρόταση μιας νέας αρχιτεκτονικής, μέχρι την πρακτική υλοποίηση, τα σενάρια χρήσης, καθώς και την αξιολόγηση της απόδοσης και της αποδοχής του συστήματος από τους χρήστες.

Οι κύριες συνεισφορές περιλαμβάνουν:

Κεφάλαιο 2: Ανασκόπηση Βιβλιογραφίας

1. Παρουσιάζει την τρέχουσα κατάσταση της τεχνολογίας αναφορικά με τα **testbeds** και τα **Cyber Range**.
2. Αναλύει τις υπάρχουσες προσεγγίσεις και τις ελλείψεις τους, εντοπίζοντας τα κενά που πρέπει να καλυφθούν.
3. Παρέχει μια σύγκριση των χαρακτηριστικών και των εργαλείων που χρησιμοποιούνται στα σύγχρονα **Cyber Range**.

Κεφάλαιο 3: Σχεδίαση **Cyber Range**

1. Προτείνει μια νέα αρχιτεκτονική για τα **Cyber Range**, βασισμένη σε ζωντανούς.
2. Περιγράφει λεπτομερώς τις απαιτήσεις και τις προδιαγραφές της αρχιτεκτονικής αυτής.

3. Προσφέρει μια ολοκληρωμένη παρουσίαση των λειτουργικών μονάδων του προτεινόμενου συστήματος.

Κεφάλαιο 4: Υλοποίηση Cyber Range

1. Εξηγεί την τεχνική υλοποίηση της προτεινόμενης αρχιτεκτονικής.
2. Συγκρίνει την υλοποίηση αυτή με υπάρχοντα συστήματα, αναδεικνύοντας τα πλεονεκτήματα της νέας προσέγγισης.
3. Παρουσιάζει τα εργαλεία και τις τεχνολογίες που χρησιμοποιήθηκαν κατά την ανάπτυξη της πλατφόρμας.

Κεφάλαιο 5: Ενίσχυση της Κυβερνοασφάλειας μέσω των Cyber Range

1. Διερευνά τη σημασία των Cyber Range στην εκπαίδευση και στην έρευνα στην κυβερνοασφάλεια.
2. Παρουσιάζει μεθόδους και τεχνικές για τη βελτίωση της εκπαιδευτικής διαδικασίας μέσω των Cyber Range.
3. Εξετάζει τη χρήση στρατηγικών συμπεριφοράς και gamification για την ενίσχυση της μάθησης.

Κεφάλαιο 6: Σενάρια Χρήσης

1. Παρουσιάζει συγκεκριμένα σενάρια χρήσης της προτεινόμενης αρχιτεκτονικής.
2. Αξιολογεί την αποτελεσματικότητα του συστήματος σε διάφορες ρεαλιστικές καταστάσεις.
3. Αναδεικνύει τις δυνατότητες και τις προκλήσεις που αντιμετωπίζονται κατά την υλοποίηση των σεναρίων.

Κεφάλαιο 7: Αξιολόγηση

1. Αναλύει την απόδοση του συστήματος μέσω σεναρίων **stress testing**.
2. Παρουσιάζει τα αποτελέσματα της αποδοχής από τους χρήστες και την αποτελεσματικότητα του συστήματος.
3. Συγκρίνει την απόδοση των **containers** με τις εικονικές μηχανές, αναδεικνύοντας τα οφέλη της προτεινόμενης αρχιτεκτονικής.

Κεφάλαιο 8: Συμπεράσματα και Μελλοντική Εργασία

1. Συνοψίζει τα ευρήματα της έρευνας και τις συνεισφορές της διατριβής.
2. Προτείνει μελλοντικές κατευθύνσεις για έρευνα με στόχο την περαιτέρω βελτίωση των τεχνολογιών **Cyber Range** και των εφαρμογών τους στην κυβερνοασφάλεια.

Κάθε κεφάλαιο είναι επιμελώς σχεδιασμένο για να αντιμετωπίσει συγκεκριμένες πτυχές της ανάπτυξης των **Cyber Range**, από τις θεωρητικές βάσεις έως την πρακτική εφαρμογή και αξιολόγηση.

Κεφάλαιο 2

Το Κεφάλαιο αυτό παρέχει μια ολοκληρωμένη εικόνα της τρέχουσας κατάστασης και των προκλήσεων που αντιμετωπίζουν τα **Cyber Range**, ενώ παράλληλα προσφέρει προτάσεις για την μελλοντική ανάπτυξη και βελτίωση τους. Το κεφάλαιο αποτελείται από 5 ενότητες.

Η πρώτη ενότητα περιλαμβάνει την ανασκοπήση διαφόρων μελετών και ερευνών σχετικών με τα **Cyber Ranges** και τα **Testbeds**. Αναφέρονται αρκετές ταξινομήσεις και κατηγοριοποιήσεις, όπως το έργο των **Davis και Magrath (2013)**, το οποίο κατηγοριοποίησε τα **Cyber Range** σε προσομοιώσεις, **ad-hoc** ή **overlay** και εξομοιώσεις, καθώς και άλλες μελέτες που εστίασαν σε συγκεκριμένους τομείς, όπως τα **ICS**.

Η μεθοδολογία αυτής της έρευνας παρουσιάζεται στην δεύτερη ενότητα και περιλαμβάνει την συστηματική αναγνώριση και κριτική ανάλυση της τρέχουσας κατάστασης των

Cyber Range. Χρησιμοποιήθηκε μια μικτή μεθοδολογία συλλογής δεδομένων, η οποία περιλαμβάνει βιβλιογραφική ανασκόπηση και δομημένες συνεντεύξεις με πανεπιστήμια και οργανισμούς που έχουν εφαρμόσει και λειτουργήσει τέτοιου είδους συστήματα.

Σε αυτή την ενότητα, παρουσιάζονται τα αποτελέσματα της έρευνας, συμπεριλαμβανομένων των στόχων των **Cyber Range**, των τομέων που υποστηρίζονται, των τύπων περιβάλλοντος και των εργαλείων υλοποίησης. Γίνεται αναφορά σε διάφορα είδη προκλήσεων ασφάλειας που αντιμετωπίζονται στα **Cyber Range**, όπως η ασφάλεια ιστού, η ψηφιακή εγκληματολογία και η ανάλυση κακόβουλου λογισμικού. Επιπλέον, εξετάζονται οι εκπαιδευτικοί σκοποί και οι τρόποι πρόσβασης στα **Cyber Range**.

Η επόμενη ενότητα συζητά τις προκλήσεις που αντιμετωπίζουν τα **Cyber Range**, όπως η διαχείριση της πολυπλοκότητας και η ανάγκη για βελτιωμένες δυνατότητες προσομοίωσης. Αναφέρονται επίσης οι μελλοντικές κατευθύνσεις για την ανάπτυξη και την εφαρμογή των **Cyber Ranges**, προτείνοντας την ενσωμάτωση νέων τεχνολογιών και την αύξηση της ρεαλιστικότητας των προσομοιώσεων.

Τα συμπεράσματα της ανασκόπησης βιβλιογραφίας συνοψίζουν την τρέχουσα κατάσταση και τις προοπτικές για τα **Cyber Range**. Αναγνωρίζονται τα κενά στη βιβλιογραφία και προτείνονται τρόποι για την κάλυψή τους μέσω περαιτέρω έρευνας και ανάπτυξης.

Κεφάλαιο 3

Στο τρίτο κεφάλαιο της διατριβής, επικεντρωνόμαστε στην προτεινόμενη αρχιτεκτονική για το σύστημα **Cyber Range**. Το κεφάλαιο ξεκινά με την περιγραφή των απαιτήσεων και των προδιαγραφών και προχωρά στην αναλυτική παρουσίαση της αρχιτεκτονικής, περιγράφοντας λεπτομερώς τις πτυχές σχεδιασμού και υλοποίησης.

Η αρχιτεκτονική του προτεινόμενου **Cyber Range** περιλαμβάνει έξι βασικές ενότητες:

1. **Web Fronted:** Λειτουργεί ως η βασική πύλη για τους χρήστες, επιτρέποντας την αλληλεπίδραση με υπηρεσίες όπως υπολογιστική ισχύς, δικτύωση, αποθήκευση, και διαχείριση σεναρίων.

2. **Storage:** Διαχειρίζεται κρίσιμα δεδομένα, όπως σενάρια, πρότυπα και αρχεία καταγραφής, επιτρέποντας την αποθήκευση και διαχείριση των σεναρίων και την ανταλλαγή τους μεταξύ διαφορετικών **Cyber Range instances**.
3. **Scenario:** Διευκολύνει τη δημιουργία, ανάπτυξη, και διαχείριση των σεναρίων κυβερνοασφάλειας, χρησιμοποιώντας πρότυπα **Heat** για την αυτόματη δημιουργία των αναγκαίων πόρων και διαμορφώσεων για κάθε άσκηση.
4. **Management:** Παρακολουθεί την κατάσταση του **Cyber Range**, περιλαμβάνοντας τη χρήση πόρων, δείκτες απόδοσης και την υγεία του συστήματος, παρέχοντας ανατροφοδότηση και βελτιώσεις βάσει των εκτελεσμένων σεναρίων.
5. **Environment:** Υποστηρίζει το λειτουργικό περιβάλλον των σεναρίων, διαχειριζόμενο τις συνθήκες εκτέλεσης και εξασφαλίζοντας την απομόνωση των δικτύων για την αποτροπή παρεμβολών μεταξύ των σεναρίων.
6. **Orchestration:** Συντονίζει την παροχή και διαχείριση των πόρων υποδομής και λογισμικού, χρησιμοποιώντας πρότυπα **Heat** και εργαλεία **Infrastructure as Code (IaC)** όπως **Ansible** για την αυτοματοποίηση των διαδικασιών κύκλου ζωής των σεναρίων, από την ανάπτυξη έως την παράδοση.

Η προτεινόμενη αρχιτεκτονική προσφέρει μια ευέλικτη και κλιμακούμενη πλατφόρμα για τη δημιουργία και διαχείριση σεναρίων κυβερνοασφάλειας. Η χρήση τεχνολογιών κοντέινερ και ανοιχτού κώδικα, όπως **Docker** και **OpenStack**, μειώνει το κόστος και βελτιστοποιεί την απόδοση, κάνοντας την πλατφόρμα προσιτή για μικρά και μεσαία πανεπιστήμια.

Η προτεινόμενη αρχιτεκτονική υποστηρίζει επίσης την ενσωμάτωση με υφιστάμενα συστήματα εκπαίδευσης και τεχνολογικής υποδομής, διευκολύνοντας τη χρήση και τη διαχείριση των σεναρίων από χρήστες με διαφορετικά επίπεδα τεχνικής εξειδίκευσης. Επιπλέον, η πλατφόρμα παρέχει προηγμένα εργαλεία παρακολούθησης και οπτικοποίησης, ενισχύοντας τη διαχείριση της υποδομής και την εμπειρία των χρηστών κατά την εκτέλεση ασκήσεων κυβερνοασφάλειας.

Συνολικά, η προτεινόμενη αρχιτεκτονική του προτεινόμενου συστήματος **Cyber Range** ενισχύει την ερευνητική ικανότητα του πανεπιστημίου, παρέχοντας ένα σύγχρονο και ρεαλιστικό περιβάλλον για την εκπαίδευση και την έρευνα στην κυβερνοασφάλεια .

Κεφάλαιο 4

Στο Κεφάλαιο 4 αναλύεται λεπτομερώς η τεχνική υλοποίηση του συστήματος **Cyber Range**. Το κεφάλαιο αυτό παρέχει μια εκτενή περιγραφή των υποδομών και των τεχνολογιών που χρησιμοποιήθηκαν για την υλοποίηση, εστιάζοντας κυρίως στις πλατφόρμες υποδομής, τις τεχνολογίες ανάπτυξης και τα πλαίσια ανάπτυξης.

Αρχικά, εξετάζονται οι υποδομές που χρησιμοποιήθηκαν, περιλαμβάνοντας πλατφόρμες όπως το **OpenStack**, που παρέχει ένα ευέλικτο και επεκτάσιμο περιβάλλον για την ανάπτυξη των **Cyber Ranges**. Αναφέρονται επίσης οι τεχνολογίες ανάπτυξης που περιλαμβάνουν εργαλεία όπως τα **Docker containers** και το **Kolla-Ansible**, τα οποία διευκολύνουν τη διαδικασία ανάπτυξης και διαχείρισης των υπηρεσιών.

Στη συνέχεια, περιγράφονται τα πλαίσια ανάπτυξης που χρησιμοποιήθηκαν για την υλοποίηση του συστήματος, όπως τα **deployment frameworks**. Ειδική αναφορά γίνεται στις τεχνολογίες ανάπτυξης και στους λόγους για την επιλογή της διανομής **Kolla-Ansible**, τονίζοντας τα πλεονεκτήματα που προσφέρει, όπως η ευκολία στη διαχείριση και η αύξηση της αποδοτικότητας.

Το κεφάλαιο εξετάζει επίσης το **Learning Management System (LMS)** που χρησιμοποιήθηκε για την υποστήριξη των εκπαιδευτικών δραστηριοτήτων, καθώς και τις δυνατότητες παρακολούθησης και ειδοποίησης, που ενισχύουν τη διαχείριση των δραστηριοτήτων και την ασφάλεια των συστημάτων.

Τέλος, παρουσιάζονται οι λειτουργικότητες και ικανότητες του συστήματος **Cyber Range**, περιγράφοντας τα βασικά χαρακτηριστικά και τις δυνατότητες που προσφέρονται στους χρήστες, διευκολύνοντας την μάθηση και την εξάσκηση σε ρεαλιστικά σενάρια κυβερνοασφάλειας.

Συνολικά, το τέταρτο κεφάλαιο παρέχει μια ολοκληρωμένη εικόνα της τεχνικής υλοποίησης του συστήματος **Cyber Range**, παρουσιάζοντας τις πλατφόρμες και τις τεχνολογίες που αξιοποιήθηκαν, καθώς και τις λειτουργικότητες που ενισχύουν την εκπαιδευτική και ερευνητική διαδικασία.

Κεφάλαιο 5

Το πέμπτο κεφάλαιο εστιάζει στην ενίσχυση της ικανότητας κυβερνοασφάλειας μέσω της χρήσης **Cyber Range**. Αναλύονται και παρουσιάζονται οι καινοτόμες μέθοδοι εκπαίδευσης και οι εφαρμογές των **Cyber Ranges** στην ακαδημαϊκή εκπαίδευση και την επαγγελματική εξέλιξη..

Τα **Cyber Ranges** παρέχουν πρακτική εκπαίδευση σε σενάρια πραγματικού κόσμου, βελτιώνοντας την τεχνική επάρκεια και την ετοιμότητα των εκπαιδευομένων για την αγορά εργασίας. Τονίζεται η χρήση της παιγνιοποίησης (**gamification**) και των ψηφιακών διδύμων (**digital twins**) για την αύξηση της αφοσίωσης και της αποτελεσματικότητας της εκπαίδευσης.

Η ενσωμάτωση στρατηγικών συμπεριφοράς στην εκπαίδευση κυβερνοασφάλειας είναι κρίσιμη για την αποτελεσματική προστασία δεδομένων. Τέτοιες στρατηγικές περιλαμβάνουν την ενίσχυση της αντίληψης απειλών. Αναλύονται επίσης οι απειλές που προέρχονται από εσωτερικούς χρήστες και οι τεχνικές και μη-τεχνικές μέθοδοι για την αναγνώριση και την αντιμετώπισή τους. Η εκπαίδευση σε αυτά τα σενάρια είναι κρίσιμη για την αντιμετώπιση αυτών των απειλών.

Η παιγνιοποίηση αναγνωρίζεται ως αποτελεσματική μέθοδος για την ενίσχυση της μάθησης στην κυβερνοασφάλεια. Οι εκπαιδευόμενοι εμπλέκονται ενεργά σε διαδραστικά και ανταγωνιστικά περιβάλλοντα, βελτιώνοντας τις δεξιότητες και την κατανόησή τους. Το κεφάλαιο αναλύει επίσης τη χρήση του Ευρωπαϊκού Πλαισίου Δεξιοτήτων Κυβερνοασφάλειας **ECSF** για την τυποποίηση και την ενίσχυση των δεξιοτήτων των επαγγελματιών του χώρου. Η ενσωμάτωση του **ECSF** στον σχεδιασμό των **Cyber Ranges** διασφαλίζει την κάλυψη των ευρωπαϊκών και διεθνών προτύπων.

Περιγράφονται διάφορες μορφές ασκήσεων κυβερνοασφάλειας, όπως οι ασκήσεις άμυνας (CDX), οι επιτραπέζιες ασκήσεις (TTX), και οι διαγωνισμοί Capture the Flag (CTF). Αυτές οι ασκήσεις είναι κρίσιμες για την ανάπτυξη τόσο τεχνικών όσο και μη-τεχνικών δεξιοτήτων.

Το πέμπτο κεφάλαιο αναδεικνύει τη σημασία των **Cyber Ranges** στην εκπαίδευση κυβερνοασφάλειας, προσφέροντας ένα πρακτικό και διαδραστικό περιβάλλον για την ανάπτυξη δεξιοτήτων. Η εφαρμογή στρατηγικών συμπεριφοράς, παιγνιοποίησης και η χρήση του ECSF είναι μερικά από τα κύρια στοιχεία που βελτιώνουν την αποτελεσματικότητα της εκπαίδευσης και ενισχύουν την ετοιμότητα των επαγγελματιών της κυβερνοασφάλειας. Με αυτές τις καινοτομίες, τα **Cyber Ranges** συμβάλλουν σημαντικά στην κάλυψη του χάσματος δεξιοτήτων στην κυβερνοασφάλεια, προετοιμάζοντας καλύτερα τους επαγγελματίες για την αντιμετώπιση σύγχρονων και μελλοντικών απειλών.

Κεφάλαιο 6

Το έκτο κεφάλαιο αναλύει και παρουσιάζει διάφορες περιπτώσεις χρήσης του προτεινόμενου συστήματος **Cyber Ranges**. Αυτά τα σενάρια δεν λειτουργούν απλώς ως εκπαιδευτικά εργαλεία, αλλά ως μέσο για την απόκτηση βαθιάς κατανόησης των προκλήσεων που αντιμετωπίζουν οι επαγγελματίες στον τομέα της κυβερνοασφάλειας. Το κεφάλαιο επιδιώκει να ενισχύσει τις δεξιότητες των συμμετεχόντων μέσα από την πρακτική εφαρμογή και την προσομοίωση πραγματικών απειλών, προετοιμάζοντάς τους έτσι για τις προκλήσεις που θα συναντήσουν στον πραγματικό κόσμο.

Τα σενάρια που παρουσιάζονται περιλαμβάνουν διάφορες προκλήσεις, όπως το σενάριο της έγχυσης κακόβουλου κώδικα σε πλατφόρμα **WordPress**, το οποίο εξετάζει την ευπάθεια σε επιθέσεις **SQL Injection**. Άλλο σενάριο εστιάζει στην ανίχνευση κακόβουλης κίνησης δικτύου, παρέχοντας στους εκπαιδευόμενους τις δεξιότητες για τον εντοπισμό και την ανάλυση ύποπτων δραστηριοτήτων. Επίσης, περιλαμβάνονται σενάρια που αφορούν την ανακάλυψη και σάρωση υποδοχών δικτύου, καθώς και προηγμένες τεχνικές σάρωσης, που επιτρέπουν στους συμμετέχοντες να κατανοήσουν καλύτερα τις μεθόδους που

χρησιμοποιούνται για την ανίχνευση και αξιολόγηση ευπαθειών. Ένα από τα σενάρια που αναλύονται αφορά την αξιολόγηση ευπαθειών που προσομοιώνει έναν μη ασφαλή ιστότοπο. Το σενάριο αυτό δίνει στους συμμετέχοντες τη δυνατότητα να εφαρμόσουν τεχνικές ανάλυσης ευπαθειών και να εντοπίσουν αδυναμίες που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι χρήστες. Τέλος, το σενάριο σάρωσης ευπαθειών σε **Docker Containers** παρέχει πρακτική εμπειρία στη χρήση τεχνολογιών **containerization**, οι οποίες είναι ολοένα και πιο σημαντικές στον σύγχρονο κόσμο της κυβερνοασφάλειας.

Το κεφάλαιο ολοκληρώνεται με συμπεράσματα, επισημαίνοντας την αποτελεσματικότητα των σεναρίων χρήσης στην ενίσχυση των δεξιοτήτων και της γνώσης των συμμετεχόντων στον τομέα της κυβερνοασφάλειας

Κεφάλαιο 7

Το έβδομο κεφάλαιο επικεντρώνεται στην αξιολόγηση της αποτελεσματικότητας και της χρηστικότητας του **Cyber Range**, όπως και στη συνολική επίδραση του στους συμμετέχοντες. Η διαδικασία αξιολόγησης περιλάμβανε αυστηρά σενάρια δοκιμών που προσομοίωναν πραγματικές συνθήκες, με σκοπό να αξιολογηθεί η απόδοση του συστήματος υπό πίεση. Αυτά τα σενάρια σχεδιάστηκαν για να εντοπιστούν τόσο τα πλεονεκτήματα όσο και οι τομείς βελτίωσης του **Cyber Range**.

Αναλυτικότερα, η ανάλυση απόδοσης του συστήματος περιλάμβανε δοκιμές στρες τεστ κατά τη διάρκεια των σεναρίων εργασίας. Η ανάλυση έδειξε ότι η χρήση τεχνολογίας **container** προσφέρει σημαντικά πλεονεκτήματα σε σχέση με τις εικονικές μηχανές (**VMs**) όσον αφορά την αποδοτικότητα πόρων και τον χρόνο υλοποίησης. Αυτή η ανάλυση βοήθησε στην βελτιστοποίηση της κατανομής πόρων και την αποφυγή της υποβάθμισης της απόδοσης.

Η αποδοχή των χρηστών εξετάστηκε μέσω της παρουσίασης και εκπαίδευσης των φοιτητών του Πανεπιστημίου Δυτικής Αττικής, που περιλάμβανε ασκήσεις εντός του πλαισίου του **Cyber Range**. Οι συμμετέχοντες είχαν την ευκαιρία να εφαρμόσουν τις γνώσεις και τις δεξιότητές τους σε ένα ελεγχόμενο περιβάλλον, επιτρέποντάς τους να

αναπτύξουν προηγμένες δεξιότητες κυβερνοασφάλειας. Ένα σημαντικό ποσοστό των συμμετεχόντων ανέφερε ότι το **Cyber Range** συνέβαλε στην ενίσχυση των γνώσεών τους σε θέματα όπως η δημιουργία και η ασφάλεια δικτύων.

Τα αποτελέσματα της έρευνας έδειξαν ότι οι συμμετέχοντες αξιολόγησαν θετικά την εμπειρία τους με το **Cyber Ranges**, υπογραμμίζοντας την αποτελεσματικότητά του στην παροχή πρακτικής εκπαίδευσης κυβερνοασφάλειας. Το 36% των συμμετεχόντων συμφώνησε έντονα και το 59% συμφώνησε ότι το **Cyber Range** θα συμβάλει στην ανάπτυξη προηγμένων δεξιοτήτων. Επίσης, προτάθηκαν βελτιώσεις όπως η προσθήκη λειτουργιών για την αναγνώριση απειλών, η ασφάλεια AI και νέα μαθήματα.

Συμπερασματικά, συνιστάται η ανάπτυξη μιας βελτιωμένης υπηρεσίας ιστού με φιλικές προς τον χρήστη λειτουργίες για την επόμενη έκδοση του **Ethaca Cyber Range**. Επιπλέον, η αξιολόγηση αποκάλυψε την ανάγκη για συνεχή βελτίωση του περιβάλλοντος χρήστη και την ενσωμάτωση νέων τεχνολογιών όπως η AI και η ασφάλεια IoT, για να διασφαλιστεί ότι το **Cyber Range** παραμένει στην αιχμή της εκπαίδευσης στην κυβερνοασφάλεια.

Το έβδομο κεφάλαιο παρουσίασε λεπτομερώς την αξιολόγηση του **Ethaca Cyber Range**, τονίζοντας τα πλεονεκτήματα και τις περιοχές βελτίωσης του συστήματος. Η θετική ανατροφοδότηση από τους συμμετέχοντες και οι προτεινόμενες βελτιώσεις παρέχουν έναν σαφή οδικό χάρτη για τη μελλοντική ανάπτυξη και ενίσχυση της πλατφόρμας, με στόχο τη βελτίωση της εκπαίδευσης στην κυβερνοασφάλεια.

Κεφάλαιο 8

Το όγδοο κεφάλαιο επικεντρώνεται στα συμπεράσματα και τις μελλοντικές κατευθύνσεις για τα συστήματα **Cyber Range** στην εκπαίδευση και έρευνα στον τομέα της κυβερνοασφάλειας. Το κεφάλαιο αυτό συνθέτει τα ευρήματα της έρευνας, παρουσιάζοντας τις τρέχουσες εξελίξεις, τις προκλήσεις, και τις προτεινόμενες λύσεις για την ανάπτυξη και βελτίωση των συστημάτων **Cyber Ranges**.

Η ανάλυση των συστημάτων **Cyber Ranges** αναδεικνύει τη σημασία της κλίμακωσης και της προσαρμοστικότητας, καθώς και της ενσωμάτωσης με εκπαιδευτικά πλαίσια.

Η συγκριτική ανάλυση των σύγχρονων αρχιτεκτονικών και πλατφορμών **Cyber Ranges** επισημαίνει τα πλεονεκτήματα των καινοτόμων λύσεων που βασίζονται σε **containers**, προσφέροντας διαδραστική και πρακτική εκπαίδευση στην κυβερνοασφάλεια. Οι αξιολογήσεις της αποδοχής από τους χρήστες υπογραμμίζουν την αποτελεσματικότητα της πλατφόρμας στην ενίσχυση των δεξιοτήτων κυβερνοασφάλειας. Τα ευρήματα αυτά δείχνουν ότι η συνεχής ανάπτυξη και βελτίωση των συστημάτων **Cyber Ranges** είναι κρίσιμη για την αντιμετώπιση των σύνθετων απειλών στον κυβερνοχώρο.

Οι μελλοντικές κατευθύνσεις για έρευνα περιλαμβάνουν την περαιτέρω ανάπτυξη και βελτίωση της αρχιτεκτονικής **Cyber Range** με βάση τις ανάγκες των χρηστών και τις εξελίξεις στον τομέα της κυβερνοασφάλειας. Ένα κρίσιμο σημείο είναι η ενσωμάτωση προηγμένων μεθόδων ανίχνευσης απειλών και μηχανισμών απόκρισης, αξιοποιώντας τεχνικές μηχανικής μάθησης και τεχνητής νοημοσύνης. Επιπλέον, η διεύρυνση των σεναρίων χρήσης για να καλύψουν νέες μορφές κυβερνοεπιθέσεων και η διερεύνηση της διαλειτουργικότητας με άλλες πλατφόρμες εκπαίδευσης και εργαλεία ανάλυσης είναι επίσης σημαντικές. Τέλος, η αξιολόγηση της επίδρασης των **gamified** τεχνικών μάθησης και η διερεύνηση της μακροπρόθεσμης αποτελεσματικότητας της εκπαίδευσης με τη χρήση των **Cyber Ranges** παραμένουν ανοικτά πεδία έρευνας.

Appendix C

Cyber Range Questionnaire

1. What is the objective of the Cyber Range? (select all that apply)
2. What is the supporting sector of the Cyber Range? (select all that apply)
3. What is the domain that is emulated or replicated in the operational environment?
(select all that apply)
4. What type of security challenges are provided? (select all that apply)
5. Is the Cyber Range used for educational purposes?
6. What is the type of Cyber Range environment?
7. Which infrastructure platform(s) is(are) used to develop the Cyber Range?
8. What type of access does it provide to participants? (select all that apply)
9. What tools are used to i. Set up Vms? ii. Set up network topology? iii. Keep scoring?
(flag dashboards, log analyzers, etc) iv. Create cyber security scenarios? v. Manage
the Cyber Range? (resources) vi. Monitoring the exercises? (SIEM, IDS, etc) vii.
Generate network traffic? viii. Generate user behavior? ix. Other functions?
10. Teams, Roles and Participants i. How many teams can participate at the same time? ii.
Total number of active participants? iii. PARTICIPANTS: What are the roles/functions?
(select all that apply) iv. Roles

11. Does the Cyber Range been used already?
12. Does the Cyber Range provide any dataset? i. if yes the dataset is? ii. What type of information do the dataset contain?

Appendix D

OpenStack Kolla-Ansible Deployment

This Appendix covers detailed instructions for implementing OpenStack with Kolla-Ansible on either physical or virtual nodes. The minimum requirements of OpenStack Kolla-Ansible AIO deployment are provided in Table 4.3.

Update/upgrade your system

```
sudo apt update
```

```
sudo apt upgrade
```

Install required packages

```
sudo apt install python3-dev libffi-dev gcc libssl-dev
```

Install Python

```
sudo apt install python python-pip
```

```
sudo apt install python3 python3-pip
```

Install pip

```
python3 -m pip install --upgrade pip
```

Create and activate virtual environment

```
source ./activate
```

```
mkdir cloud
```

```
cd cloud
```

```
cd ..
```

```
rm -rfd cloud
```

```
sudo apt install virtualenv
virtualenv -p /usr/bin/python3 cloudv
cd cloudv
```

Install and Configure Ansible

```
pip install ansible
vi /etc/ansible/ansible.cfg
[defaults]
host_key_checking=False
pipelining=True
forks=100
```

Install and Configure Kolla-Ansible for AIO Deployment

```
source ./activate
pip install git+https://opendev.org/openstack/kolla-ansible@master
sudo mkdir -p /etc/kolla
sudo chown USER :USER -R /etc/kolla
cd kolla-ansible
cd share/kolla-ansible/etc_examples/kolla/globals.yml /etc/kolla/
cp share/kolla-ansible/etc_examples/kolla/globals.yml /etc/kolla/
cp share/kolla-ansible/etc_examples/kolla/passwords.yml /etc/kolla/
cp -r ./share/kolla-ansible/etc_examples/kolla/* /etc/kolla
cp -r ./share/kolla-ansible/ansible/inventory/all-in-one /etc/kolla
cp -r ./share/kolla-ansible/ansible/inventory/multinode /etc/kolla
git clone --branch master https://opendev.org/openstack/kolla-ansible
kolla-ansible install-deps
mkdir -p /etc/ansible
sudo mkdir -p /etc/ansible
```

Configure global deployment options

```
vi /etc/kolla/globals.yml
workaround_ansible_issue_8743: "yes"
```



```
kolla_base_distro: "ubuntu"
kolla_install_type: "source"
kolla_internal_vip_address: "xxx.xxx.xxx.xxx"
network_interface: "ens160"
neutron_external_interface: "ens224"
openstack_release: "zed"
enable_cinder: "yes"
enable_cinder_backend_lvm: "yes"
cinder_volume_group: "cinder-volume"
enable_zun: "yes"
enable_kuryr: "yes"
enable_etcd: "yes"
Docker_configure_for_zun: "yes"
containerd_configure_for_zun: "yes"
nova_compute_virt_type: "qemu"
enable_neutron_provider_networks: "yes"
enable_openstack_core: "yes"
```

Generate Passwords for Kolla

```
kolla-genpwd
```

```
cd cloudv/
```

Deploy Kolla-Ansible Inventory

```
cd /etc/kolla
```

```
kolla-ansible -i all-in-one bootstrap-servers
```

```
kolla-ansible -i all-in-one prechecks
```

```
kolla-ansible -i all-in-one deploy
```

```
/cloudv/share/kolla-ansible/init-runonce
```

```
openstack server create --image cirros --flavor m1.tiny --key-name mykey --network demo-
```

```
net demo1
```

```
cloud-env
```

```
pip install python-openstackclient python-neutronclient python-glanceclient
```

Generate OpenStack admin credentials file

```
source /etc/kolla/admin-openrc.sh
```

```
kolla-ansible post-deploy
```

List of running OpenStack Docker containers

```
sudo Docker ps
```

List of Openstack networks

```
openstack network list
```

List of OpenStack service

```
openstack service list
```

Appendix E

Cyber Range Questionnaire

The objective of our interview is to scrutinize participants' perceptions of the Uniwa Cyber Range. Our goal is to foster practical knowledge and skills in cybersecurity within a hands-on learning environment, imparting participants with a thorough understanding of the tools utilized by cybersecurity professionals and potential threat actors.

1. How many years have you been involved in cybersecurity? (select all that apply)

- 0-1
- 2-4
- 5-6
- 7-9
- 10+
- 15+
- Other

2. Have you participated in cybersecurity exercises in the past?

- Yes
- No

3. If you answered yes, in what type of cybersecurity exercises have you participated?
(select all that apply)

- CTF
- Table Top
- Red /Blue Team
- Cyber Range
- Other

4. Have you previously engaged with or utilized a Cyber Range as part of your professional or educational experience? (select all that apply)

- Yes
- No

5. What are the main categories of cybersecurity that you would like the Cyber Range to cover?

- Web Security
- Network Security
- Software Security
- System Security
- Social engineering
- Threat Intelligence
- Cryptography
- Red Blue Team

6. Please answer the following questions based on your experience with UNIWA Cyber Range. (Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree)

Does it contribute:

- to the development of advanced skills and strategies in the field of cybersecurity?
 - to expand knowledge concerning infrastructure components, such as servers, storage, and cloud services?
 - to the advancement of knowledge regarding the creation, management, and security of networks?
 - to promote knowledge in programming and software development?
 - to streamline the process by reducing the execution time needed for creating cybersecurity exercises?
7. How important do you think it is for Uniwa to incorporate a Cyber Range for its students to enhance their technical cybersecurity knowledge?
- Very important
 - Important
 - Fairly important
 - Slightly Important
 - Not at all important
8. What additional features or capabilities would you like to see in the Uniwa Cyber Range to make it more useful for your educational or research needs?
9. How would you assess the working environment of the Uniwa Cyber Range?
- Very Satisfied
 - Satisfied
 - Neither Satisfied/Dissatisfied
 - Dissatisfied
 - Very Dissatisfied
10. Overall, how helpful did you find the experience at Uniwa Cyber Range?

- Extremely Helpful
- Very Helpful
- Neither Helpful nor Unhelpful
- Very Unhelpful
- Extremely Unhelpful

Appendix F

Cybersecurity Exercise Template for Cyber Range System

Exercise Overview

- **Title:** Choose a concise title that reflects the essence of the exercise.
- **Date and Time:** Schedule when the exercise will take place.
- **Duration:** Estimate how long the exercise will run.
- **Objective(s):** Clearly define what the exercise aims to achieve (e.g., enhancing incident response skills, identifying vulnerabilities, etc.).

2. Target Audience

- **Participants:** List the roles who should participate (e.g., network administrators, cybersecurity analysts, etc.).
- **Prerequisites:** Specify the required or expected skill level of participants (beginner, intermediate, advanced).

3. Exercise Scenario(s)

- **Background:** Provide a brief description of the exercise.

- **Threats and Vulnerabilities:** Describe the specific cybersecurity threats and vulnerabilities that participants will address.

4. Infrastructure and Resources

- **Cyber Range Environment:** Describe the cyber range setup, including resource specifications such as networking configurations, and any OS images, containers, CPU, memory, and storage used.
- **Tools and Technologies:** List any specific tools, software, or technologies that participants will use or encounter during the exercise.
- **Supporting Materials:** Mention any guides, or documentation provided to participants.

5. Exercise Conduct

- **Roles and Responsibilities:** Define the roles of facilitators, observers, and participants. Clarify what is expected from each role.
- **Rules of Engagement:** Set the boundaries for the exercise, including what is allowed and what is off-limits.

6. Evaluation criteria and Feedback

- **Success Criteria:** Define how the success of the exercise will be measured (e.g., specific objectives met, vulnerabilities identified).
- **Feedback Mechanism:** Describe how participants can provide feedback on the exercise experience.