

**A Cybersecurity Skills Performance Dashboard (CSPD):
The Use of a Technical Gamification Simulation Platform
(TGSP) to Address Cybersecurity Skills Gap in the UAE**

اللوحة المعلوماتية لعرض أداء مهارات الأمن السيبراني: استخدام منصة محاكاة
الألعاب التقنية لمعالجة فجوة مهارات الأمن السيبراني في الإمارات العربية المتحدة

by

FATMA AHMAD BAZARGAN

**A thesis submitted in fulfilment
of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE
at
The British University in Dubai**

October 2021

A Cybersecurity Skills Performance Dashboard (CSPD): The Use of a Technical Gamification Simulation Platform (TGSP) to Address Cybersecurity Skills Gap in the UAE

اللوحة المعلوماتية لعرض أداء مهارات الأمن السيبراني: استخدام منصة محاكاة الألعاب التقنية
لمعالجة فجوة مهارات الأمن السيبراني في الإمارات العربية المتحدة

by

FATMA AHMAD BAZARGAN
20197440

Thesis Supervisor
Dr. Cornelius Ncube

Approved for award:

Name
Designation

Name
Designation

Name
Designation

Name
Designation

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Fatma Bazargan

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

ABSTRACT

Cybersecurity capacity building has been one of the main pillars of the UAE cybersecurity strategy to shorten the cybersecurity skills gap in the UAE. There have been several capacity building initiatives introduced by the UAE government to upscale the hands-on technical skills amongst cybersecurity professionals in the UAE.

However, there has not been any mechanism nor a platform in place to either measure the scale of the skills gap that currently exist and needs to be addressed nor any measurement tool to provide visibility into the effectiveness of the capacity building initiatives introduced. Furthermore, there have been a plethora of undergraduate cybersecurity academic degree programs taught in various recognized educational institutions across the UAE. However, the shortage of cybersecurity practitioners globally and locally has never been more acute.

Hence, there is a crucial need to introduce a UAE nation-wide cybersecurity skills performance dashboard that shall provide the required visibility into the scale of the skills gap that currently exists, hands-on technical skills that is currently available, and those skills that need to be developed and trained.

The Cybersecurity Skills Performance Dashboard (CSPD) shall provide the true measurement of the current existent skills gap shortage in the UAE to enable the concerned entities to introduce the needed capacity building initiatives to shorten the skills gap.

In addition, there is a heightened need to introduce new ways of instructing cybersecurity academic program to upscale the hands-on technical cybersecurity skills amongst university undergraduate students and thus improve a variety of technical skills such as digital forensics, incident response, reverse engineering, cryptography, penetration testing, and many more.

This research study aims to design and develop the Cybersecurity Skills Performance Dashboard (CSPD) as a measurement tool for capacity building of cybersecurity professionals. It records and provides a true assessment of the upscale of hands-on technical cybersecurity skills of cybersecurity professionals. This is fulfilled through the introduction of new ways to the current traditional academic teaching model through the use of the Technical Gamification Simulation Platform (TGSP) to shorten the cybersecurity skills gap problem in the United Arab Emirates. Integrating the TGSP within the fabric of the undergraduate cybersecurity academic programs will produce market-ready professionals to fill in the active cybersecurity job postings in the United Arab Emirates or globally.

This study employs a qualitative grounded theory research design to understand and explore how the use of the technical gamification simulation platform will enhance the hands-on technical skills amongst undergraduate students. Purposeful sampling was used to mindfully select the sample for this research work from a pool of 3rd and 4th-year undergraduate students majoring in cybersecurity from various renowned universities across the United Arab Emirates.

This research work that applied to the selected participants consisted of three phases: assess, train, and perform. The data was collected from all the three phases. The first phase, the assessment

phase, was in the form of responses to one-on-one interview questions. The second phase, which was the training phase, was in the form of results collected from the cybersecurity skills performance dashboard that was designed and developed by the researcher. Finally, the performance phase involved results that were in the form of responses to the post-training survey questionnaire by the participants in the study.

Analysis and findings indicated that the undergraduate students found the technical gamification simulation platform an invaluable tool to upscale their hands-on technical skills because it provided them with a simulated real-world environment whilst using real-world tools to complete the technical scenario in a structured manner.

This research work is considered to be the first to be conducted in the United Arab Emirates that examined providing undergraduate students majoring in cybersecurity with access to the technical gamification simulation platform for a duration of 8-weeks. Also, it was able to draw invaluable information on the effectiveness of introducing the training platform alongside the academic curriculum to upscale the hands-on technical skills. Several research questions were tested as part of this research work within the U.A.E. context.

Finally, this thesis delivers the design and development of the cybersecurity skills performance dashboard (CSPD) as a measurement tool for capacity building of cybersecurity professionals and a contribution to this research study. The CSPD captures and displays the scores of the students as they complete a given technical scenario or challenge in the technical gamification simulation platform. Hence, the dashboard provides a true assessment of the cybersecurity undergraduate's technical hands-on skills.

The CSPD provides the required means to various entities (i.e., government entities, private sector, business owners, etc.) to approach the cybersecurity professional based on the skills they most need through the use of CSPD. The beneficiaries of this dashboard include entities in the UAE and worldwide.

In addition, the dashboard can be used as a reference by the U.A.E. cybersecurity policymakers to understand the cybersecurity skills that are widely available in the United Arab Emirates and the skills that further need to be trained and developed. Hence, being able to tailor the capacity building campaigns on factual data.

Also, the dashboard can act as a nationwide cybersecurity skills performance database/repository in the United Arab Emirates to understand the current availability of cybersecurity professionals and talents.

Although the dashboard in this research work is applied to the field of cybersecurity. However, it can be generalized and applied to any other field of expertise to gain invaluable insights into the skills gap.

Keywords: cybersecurity skills shortage, skills gap, capacity building, workforce development, training, gamification, simulation, cybersecurity

ABSTRACT (Arabic)

بناء القدرات في مجال الأمن السيبراني تعتبر أحد الركائز الأساسية لإستراتيجية دولة الإمارات للأمن السيبراني لمعالجة فجوة مهارات الأمن السيبراني في دولة الإمارات العربية المتحدة .كانت هناك العديد من المبادرات لبناء القدرات التي قدمتها حكومة الإمارات العربية المتحدة للارتقاء بالمهارات الفنية العملية بين المتخصصين في الأمن السيبراني في الإمارات العربية المتحدة. ومع ذلك، لم تكن هناك أي آلية أو منصة مطبقة إما لقياس حجم فجوة المهارات الموجودة حاليًا والتي تحتاج إلى معالجة أو أي أداة قياس لتوفير رؤية حول فعالية مبادرات بناء القدرات التي تم تقديمها.

علاوة على ذلك، كان هناك عدد كبير من برامج الدرجة الأكاديمية للأمن السيبراني للطلاب الجامعيين والتي يتم تدريسها في العديد من المؤسسات التعليمية المعترف بها في جميع أنحاء دولة الإمارات العربية المتحدة. ومع ذلك، فإن النقص في ممارسي الأمن السيبراني عالميًا ومحليًا لم يكن أكثر حدة من أي وقت مضى.

ومن ثم، هناك حاجة ماسة لتقديم لوحة معلومات أداء مهارات الأمن السيبراني على مستوى دولة الإمارات العربية المتحدة والتي من شأنها توفير الرؤية المطلوبة لحجم فجوة المهارات الموجودة حاليًا، والمهارات التقنية العملية المتوفرة حاليًا، وتلك المهارات التي تحتاجها ليتم تطويرها وتدريبها.

ستوفر لوحة معلومات أداء مهارات الأمن السيبراني (CSPD) المقياس الحقيقي لمعالجة فجوة المهارات الحالي في دولة الإمارات العربية المتحدة لتمكين الجهات المعنية من تقديم مبادرات بناء القدرات اللازمة لتقليص فجوة المهارات.

بالإضافة إلى ذلك، هناك حاجة متزايدة لإدخال طرق جديدة لتوجيه البرنامج الأكاديمي للأمن السيبراني للارتقاء بالمهارات العملية للأمن السيبراني بين طلاب الجامعات الجامعيين وبالتالي تحسين مجموعة متنوعة من المهارات التقنية مثل الطب الشرعي الرقمي والاستجابة للحوادث والهندسة العكسية والتشفير واختبار الاختراق وغير ذلك الكثير.

تهدف هذه الدراسة البحثية إلى تصميم وتطوير لوحة معلومات أداء مهارات الأمن السيبراني (CSPD) كأداة قياس لبناء القدرات لمتخصصي الأمن السيبراني. لوحة المعلومات ستسجل وتقدم تقييمًا حقيقيًا لمستوى التدريب العملي على مهارات الأمن السيبراني الفنية لمتخصصي الأمن السيبراني. يتم تحقيق ذلك من خلال إدخال طرق جديدة إلى نموذج التدريس الأكاديمي التقليدي الحالي من خلال استخدام منصة محاكاة الألعاب الفنية (TGSP) لتضييق مشكلة فجوة مهارات الأمن السيبراني في دولة الإمارات العربية المتحدة. سيؤدي دمج TGSP في نسيج البرامج الأكاديمية للأمن السيبراني للجامعة إلى إنتاج مهنيين جاهزين للسوق لملء الوظائف الشاغرة في مجال الأمن السيبراني في الإمارات العربية المتحدة أو على مستوى العالم.

تستخدم هذه الدراسة تصميمًا بحثيًا نوعيًا قائمًا على أسس نظرية لفهم واستكشاف كيف أن استخدام منصة محاكاة التحفيز التقني سيعزز المهارات الفنية العملية بين الطلاب الجامعيين. تم أخذ العينات الهادفة لاختيار عينة لهذا العمل البحثي بعناية من مجموعة من طلاب السنة الثالثة والرابعة الجامعيين المتخصصين في الأمن السيبراني من مختلف الجامعات المشهورة في جميع أنحاء الإمارات العربية المتحدة.

يتكون هذا العمل البحثي الذي تم تطبيقه على المشاركين المختارين من ثلاث مراحل: التقييم والتدريب والأداء. تم جمع البيانات من جميع المراحل الثلاث. كانت المرحلة الأولى، مرحلة التقييم، في شكل ردود على أسئلة المقابلة الفردية. أما المرحلة الثانية، وهي مرحلة التدريب، فكانت على شكل نتائج تم جمعها من لوحة معلومات أداء مهارات الأمن السيبراني التي صممها الباحث وطورها. أخيرًا، تضمنت مرحلة الأداء النتائج التي كانت على شكل ردود على استبيان مسح ما بعد التدريب من قبل المشاركين في الدراسة.

أشارت التحليلات والنتائج إلى أن الطلاب الجامعيين وجدوا أن منصة محاكاة الألعاب التقنية أداة لا تقدر بثمن لترقية مهاراتهم الفنية العملية لأنها زودتهم ببيئة واقعية محاكية أثناء استخدام أدوات العالم الحقيقي لإكمال السيناريو التقني في هيكل منظم.

يعتبر هذا العمل البحثي هو الأول الذي يتم إجراؤه في دولة الإمارات العربية المتحدة والذي استهدف تزويد الطلاب الجامعيين المتخصصين في الأمن السيبراني بإمكانية الوصول إلى منصة محاكاة الألعاب التقنية لمدة 8 أسابيع. كما أنه كان قادرًا على استخلاص معلومات لا تقدر بثمن حول فعالية تقديم منصة التدريب جنبًا إلى جنب مع المناهج الأكاديمية للارتقاء بالمهارات الفنية العملية. تم اختبار العديد من الأسئلة البحثية كجزء من هذا العمل البحثي داخل دولة الإمارات العربية المتحدة.

أخيرًا، تقدم هذه الأطروحة تصميم وتطوير لوحة معلومات أداء مهارات الأمن السيبراني (CSPD) كأداة قياس لبناء قدرات متخصصة في الأمن السيبراني ومساهمة في هذه الدراسة البحثية. يلتقط CSPD ويعرض درجات الطلاب أثناء إكمالهم لسيناريو تقني معين أو تحدٍ في منصة محاكاة الألعاب التقنية. ومن ثم، توفر لوحة القيادة تقييمًا حقيقيًا لمهارات التدريب العملي الفنية للطلاب الجامعيين في مجال الأمن السيبراني.

يوفر CSPD الوسائل المطلوبة للعديد من الكيانات (مثل الكيانات الحكومية والقطاع الخاص وأصحاب الأعمال، وما إلى ذلك) للتواصل مع متخصص الأمن السيبراني بناءً على المهارات التي يحتاجون إليها بشدة من خلال استخدام لوحة المعلومات، يشمل المستفيدون من لوحة التحكم هذه كيانات في دولة الإمارات العربية المتحدة وفي جميع أنحاء العالم.

بالإضافة إلى ذلك، يمكن استخدام لوحة القيادة كمرجع من قبل دولة الإمارات العربية المتحدة صناع سياسات الأمن السيبراني لفهم مهارات الأمن السيبراني المتوفرة على نطاق واسع في دولة الإمارات العربية المتحدة والمهارات التي تحتاج إلى مزيد من التدريب والتطوير. ومن ثم، القدرة على تكييف حملات بناء القدرات على أساس البيانات الواقعية.

أيضًا، يمكن أن تعمل لوحة القيادة كقاعدة بيانات / مستودع لأداء مهارات الأمن السيبراني على مستوى الدولة في دولة الإمارات العربية المتحدة لفهم التوافر الحالي لمتخصصي ومواهب الأمن السيبراني. على الرغم من أن لوحة القيادة في هذا البحث يتم تطبيقها في مجال الأمن السيبراني. ومع ذلك، يمكن تعميمها وتطبيقها على أي مجال خبرة آخر لاكتساب رؤى لا تقدر بثمن في فجوة المهارات.

الكلمات المفتاحية: نقص مهارات الأمن السيبراني، فجوة المهارات، بناء القدرات، تنمية القوى العاملة، التدريب، المحاكاة، الأمن السيبراني.

DEDICATION

I dedicate my PhD dissertation work to my family. I quote Winston Churchill here, “*there is no doubt that it is around the family and the home that all the greatest virtues are created, strengthened and maintained.*” My family has been a constant source of support and continuous strength to achieve the apparently impossible missions that I faced in my life. First and foremost, I extend my sincere gratitude to my dear mother who constantly instilled in me the importance of pursuing my education and advancing it. From Bachelors, to double Masters and now this thesis work. She repeatedly advised me to be the best version of myself and work hard for everything I aspire to achieve.

I would also like to thank the gracious support of my family members and my dear friends who believed in me and trusted me that even if I took longer than I should, I would finish this work one day. They have constantly checked on me to ensure I am on the right path and have not lost the sight of the final goal. Quitting and giving up on this work was not an option under any circumstance.

I would like to dedicate this thesis work to my dear husband, for his endless words of encouragement, support and love. Without his constant support none of this work would have been possible. He was there to support me when I hit rock bottom and did not believe in myself to complete this thesis work. He was there to lift me up through all my despair, dark hours, mental fears, many tears and when I doubted my true self. His continuous encouragement was instrumental in enabling me to complete this thesis work. He taught me that anything was possible with determination, dedication, and persistence.

Last but not the least, I would like to dedicate this thesis work to my daughter, Shaikha, for being such a joy to my life. Seeing her encouraged me to complete this thesis. I wanted her to realize the importance of continued education by seeing her mother accomplish it.

This thesis journey has not been easy for me, it had its ups and downs throughout the last several years. There is no more joy I have today than the joy of achieving this milestone. Now that I have completed on this delightful journey it is time to set a new challenge and embark on it.

ACKNOWLEDGMENT

First and foremost, my heartfelt thanks to Allah the almighty, for showering me with endless blessings throughout my life.

I would like to express my sincere gratitude to my esteemed supervisor, Dr. Cornelius Ncube for his constant assistance at every stage of this thesis work. Without his invaluable supervision and tutelage, I would not have been able to finish this work. His continuous asks of an effective and efficient work combined with his willingness to help; created a highly motivating PhD work environment for me. He always had an ear to listen and provide insightful comments and suggestions. I am grateful for the opportunity to work on this thesis with him.

I would also like to extend my special thanks to Prof. Abdulla Al Shamsi for being the perfect example of a kind and supportive vice chancellor who is always around for any help or assistance. Also, I would like to offer my sincere thanks to Prof. Khaled Shalaan and Prof. Sherif Abdulla for their invaluable feedback and comments of this work.

In addition, I would like to offer my special thanks to all the participants who contributed in this research work. Without their passion, dedication and willingness to offer support none of this work would have been possible.

Finally, my gratitude extends to the entire staff of British University in Dubai, in particular Ms. Christine Salvador for their constant support throughout this PhD journey. Many thanks to you all.

Table of Contents

DECLARATION	
COPYRIGHT AND INFORMATION TO USERS	
ABSTRACT.....	
ABSTRACT (Arabic)	
DEDICATION.....	
ACKNOWLEDGMENT	
Chapter 1: INTRODUCTION	1
1.1 Background of the Study	1
1.2 Introduction to the Problem.....	4
1.2.1 IPSOS MORI Research.....	5
1.2.2 EMSI, ESG and ISSA Research.....	5
1.2.3 Cybersecurity Ventures Research.....	5
1.2.4 MIT Technology Review.....	6
1.3 UAE Cybersecurity Educational Programs.....	7
1.4 Capacity Building: UAE Cybersecurity Strategy	9
1.5 aeCERT and ADDA Cybersecurity Workforce Framework.....	10
1.6 Statement of the Problem	12
1.7 Purpose of the Study	14
1.8 Scope of the Study	15
1.9 Research Objectives and Significance.....	17
1.10 Research Questions	21
1.11 Assumptions and Threats to Validity.....	22
1.12 Thesis Key Contributions.....	24
1.13 Chapter Summary	27
1.14 Outline of the Thesis Chapters	27
Chapter 2: LITERATURE REVIEW	30
2.1 Understanding Cybersecurity.....	32
2.2 Fundamental Elements of Cybersecurity	33
2.3 Cybersecurity threat Landscape	34
2.4 Recent Cyber Attacks	37
2.4.1 Data Breaches	37
2.4.2 Ransomwares	39

2.4.3 Supply Chain Attacks	40
2.5 The Impact of COVID-19	40
2.6 Cyberthreat Statistics.....	41
2.7 Cyberthreat Landscape in the UAE.....	42
2.8 UAE National Cybersecurity Strategy	43
2.9 UAE Cybersecurity Workforce Framework.....	44
2.10 UAE Cybersecurity Landscape Review	46
2.11 Cybersecurity Workforce Skills and Demand	47
2.12 Cybersecurity Skills Shortage	49
2.13 Current Solutions for Cybersecurity Skills Gap	55
2.14 Current Research Efforts to Bridge the Cybersecurity Skills Gap.....	57
2.14.1 Gamification	57
2.14.2 Apprenticeship	59
2.14.3 Capture the Flag Platform	60
2.14.4 Simulation	61
2.15 Current Research Gaps in filling the Cybersecurity Skills Gap and its Remedial Approaches	62
2.16 Theoretical and Conceptual Framework	63
2.17 Chapter Summary	66
Chapter 3: RESEARCH METHODOLOGY.....	68
3.1 Research Design.....	68
3.2 Grounded Theory Design	74
3.3 Population and Sample Size.....	76
3.3.1 Population and Target Population	76
3.3.2 Participant Selection	77
3.4 Research Experiment	81
3.4.1 Phase 1 – Assessment Phase.....	81
3.4.2 Phase 2 – Training Phase	82
3.4.3 Phase 3 – Performance Phase.....	83
3.5 Technical Gamification Simulation Platform and Training Scenarios and Challenges	84
3.5.1 Cyber Range Platform – Battle Room 9: Digital Forensics	85
3.5.2 Cyber Range Platform – Mission 8: ICS/SCADA, Networking and Incident Response	86
3.6 Capture the Flag Platform.....	88
3.6.1 Web Exploitation Attack	89

3.6.2 Reverse Engineering.....	90
3.6.3 Digital Forensics.....	91
3.6.4 Open-Source Intelligence (OSINT).....	92
3.6.5 Cryptography	93
3.6.6 PWN	94
3.7 Scope of the Research Work.....	95
3.8 Data Collection	95
3.8.1 Data Collection through Survey Interviews	98
3.8.2 Data Collection through Survey Questionnaire	99
3.8.3 Data Collection through think-aloud approach.....	100
3.9 Data Analysis	101
3.9.1. Data Cleaning	102
3.9.2. Data Organization and Preparation	102
3.9.3. Data Coding	103
3.9.4. Qualitative Data Analysis	103
3.10 Validity and Reliability	105
3.11 Ethical Consideration.....	105
3.12 Summary	106
Chapter 4: HANDS ON EXPERIMENT RESULTS	107
4.1 Responses from the One-on-One Interview Questions.....	110
4.1.1 Assess: Current Technical Skills	110
4.1.2 Assess: Current Confidence Level	110
4.1.3 Assess: Usage of Gamification Platform at University	111
4.1.4 Purpose of Assessment Phase	111
4.2 Responses from the Post-Training Questionnaire.....	112
4.2.1 Post Train: Knowledge Gained.....	113
4.2.2 Post Train: Skills Gained – Cyber Range	115
4.2.3 Post Train: Skills Gained – Capture the Flag.....	119
4.2.4 Post Train: Confidence Level	121
4.2.5 Post Train: Proficiency Level.....	125
4.2.6 Post Train: Development and Abilities Level	126
4.2.7 Post Train: Suggestions and Feedback.....	130
4.2.8 Post Train: Platform Preference	132
4.3 Summary	133

Chapter 5: DESIGN AND DEVELOPMENT OF CYBERSECURITY SKILLS PERFORMANCE DASHBOARD	134
5.1 Development of the Dashboard App	135
5.2 Architectural Diagram of the Dashboard	136
5.2.1 Skills Performance Dashboard Stakeholders	137
5.2.2 Architectural Diagram for CS Skills Performance Dashboard	138
5.2.3 CS Skills Performance Dashboard – Scenario Walkthrough	146
5.3 Description of the Internal Programming.....	148
5.3.1 Scripting in Visual Basic Editor.....	148
5.3.2 List of Global Variables	151
5.3.3 Navigation Procedures	154
5.3.4 Pivot Tables	156
5.4 Components of the Dashboard App.....	157
5.4.1 Main Dashboard Feature.....	157
5.4.2 Individual Dashboard Feature	162
5.4.3 Evaluation Diagram Feature.....	163
5.4.4 Scenario Description Feature	165
5.4.5 Scoring Server Feature	167
5.4.6 Challenges List Feature	168
5.4.7 Participant Form Feature.....	170
5.5 Validation of the Cybersecurity Skills Performance Dashboard.....	171
5.5.1 Participant 1 Skills Performance Evaluation	171
5.5.2 Participant 2 Skills Performance Evaluation	173
5.5.3 Participant 3 Skills Performance Evaluation	175
5.5.4 Participant 4 Skills Performance Evaluation	177
5.5.5 Participant 5 Skills Performance Evaluation	179
5.5.6 Participant 6 Skills Performance Evaluation	181
5.5.7 Participant 7 Skills Performance Evaluation	183
5.5.8 Participant 8 Skills Performance Evaluation	185
5.5.9 Participant 9 Skills Performance Evaluation	187
5.6 Summary	190
6. CONCLUSION, FINDINGS, AND RECOMMENDATIONS	191
6.1 Key Research Findings.....	192
6.2 Recommendations.....	195
6.3 Contribution to Knowledge.....	197

6.4 Usability of the Dashboard to the Industry	198
6.5 Research Implication	199
6.6 Threats to Validity	199
6.7 Future Works	201
6.8 Conclusion.....	201
REFERENCES	204
APPENDICES	217
Appendix 1: Interview Question's Template – Participant Selection for the Study	217
Appendix 2: Cyber Range – Circadence – Project Ares.....	218
Appendix 3: Cyber Range – Battle Rooms 9 and Mission 8 – Scenario Description	220
Appendix 4: Experiment Program – Calendar Breakdown	221
Appendix 5: Cyber Range: BR9 and M8 – Exported Results from Project Ares	222
Appendix 6: Post-Train Survey Questionnaire – Template.....	226
Appendix 7: Post-Train Survey Questionnaire – Participants Responses	233
Appendix 8: Skills Performance Dashboard Scores of Participants	248
Appendix 9: MAXQDA – Survey Questionnaire – Qualitative Data Analysis	259

Table of Figures

Figure 1: ISC2 2018 Study of Cybersecurity skills shortage around the globe of nearly 3 million professionals	6
Figure 2: Cyber Range – Mission 8 scenario.....	87
Figure 3: Example of capturing the flag in web-based training.....	90
Figure 4: Decompiled code into pseudocode.....	91
Figure 5: CTF Digital Forensics: L00k challenge	92
Figure 6: CTF OSINT: Trail of 404s challenge.....	93
Figure 7: CTF Cryptography: Kryptonite challenge	94
Figure 8: Informed Consent of Participants as Response to Post-Training Questionnaire	113
Figure 9: Knowledge gained from the experiment stretched the 8 weeks	114
Figure 10: Responses from participants on the open-ended question about additional knowledge gained	115
Figure 11: Participants responses on the Cyber Range platform	116
Figure 12: Participants responses to the open-ended question in regards to the additional skills learnt.	117
Figure 13: Participants' responses to the skills gained working on CTF platform	120
Figure 14: Participants' responses in regards to their confidence level of their technical skills while working on TGSP	121
Figure 15: Participants responses on their continuation of the use of TGSP	123
Figure 16: Participants' responses to the overall hands-on experience to both CR and CTF platforms..	125
Figure 17: Participants' responses to rating their proficiency level after experiencing CR and CTF platform	126
Figure 18: Participants responses to the important elements that increased the level of hands-on technical skills	128
Figure 19: Participants responses to the important elements of the TGSP.....	131
Figure 20: Cybersecurity Skills Performance Dashboard App - Main Panel	136
Figure 21: Enabling Macros for Dashboard App.....	136
Figure 22: Cybersecurity Skills Performance Dashboard Stakeholders	137
Figure 23: System Context Diagram for CS Skills Performance Dashboard.....	139
Figure 24: Container Diagram for Scoring Server	141
Figure 25: Container Diagram for Skills Dashboard	142
Figure 26: Component Diagram for Skills Dashboard - API Application	143
Figure 27: Architectural Operating Diagram Skills Performance Dashboard	145
Figure 28: Dashboard App - Visual Basic Editor	148
Figure 29: Dashboard App - Mod1_Main Program.....	149
Figure 30: Dashboard App - Commands and Comments.....	150
Figure 31: List of Global Variables	151

Figure 32: Procedure "Global_Variables"	151
Figure 33: Procedure "Load_All_Participants"	152
Figure 34: Function "Find_Scenario"	153
Figure 35: Function "LineBreak"	154
Figure 36: Navigation Procedures	155
Figure 37: Pivot Tables	156
Figure 38: Filters – Slicers	157
Figure 39: Main Menu - Dashboard App.....	158
Figure 40: Dashboard App - Update Participant Data	159
Figure 41: Dashboard App - Dashboard View	160
Figure 42: Dashboard App - Dashboard Visualization Statistics	161
Figure 43: Dashboard App - Back to Menu Button	161
Figure 44: Dashboard App - Individual Dashboard View.....	162
Figure 45: Dashboard App - Individual Dashboard View - Loaded.....	163
Figure 46: Dashboard App - Evaluation Diagram	164
Figure 47: Dashboard App - Evaluation Diagram - Loaded.....	165
Figure 48: Dashboard App - Scenario Description	166
Figure 49: Dashboard App - Scenario Description - Loaded.....	166
Figure 50: Dashboard App - Scoring Server.....	167
Figure 51: Dashboard App - Scoring Server - Loaded	168
Figure 52: Dashboard App - Challenges List.....	169
Figure 53: Dashboard App - Challenges List - Loaded.....	169
Figure 54: Dashboard App - Participant Form	170
Figure 55: Participant 1 Cybersecurity Skills Performance Level	172
Figure 56: Participant 1 Training Platform Scores and Outcomes.....	173
Figure 57: Participant 2 Cybersecurity Skills Performance Level	174
Figure 58: Participant 2 Training Platform Scores and Outcomes.....	175
Figure 59: Participant 3 Cybersecurity Skills Performance Level	176
Figure 60: Participant 3 Training Platform Scores and Outcomes.....	177
Figure 61: Participant 4 Cybersecurity Skills Performance Level	178
Figure 62: Participant 4 Training Platform Scores and Outcomes.....	179
Figure 63: Participant 5 Cybersecurity Skills Performance Level	180
Figure 64: Participant 5 Training Platform Scores and Outcomes.....	181
Figure 65: Participant 6 Cybersecurity Skills Performance Level	182
Figure 66: Participant 6 Training Platform Scores and Outcomes.....	183
Figure 67: Participant 7 Cybersecurity Skills Performance Level	184
Figure 68: Participant 7 Training Platform Scores and Outcomes.....	185

Figure 69: Participant 8 Cybersecurity Skills Performance Level	186
Figure 70: Participant 8 Training Platform Scores and Outcomes.....	187
Figure 71: Participant 9 Cybersecurity Skills Performance Level	188
Figure 72: Participant 9 Training Platform Scores and Outcomes.....	189

Chapter 1: INTRODUCTION

This chapter shall present the background of the research work, along with research aims and objectives. It will also state the research problem that needs to be addressed and its significance focused towards the UAE environment. The chapter will also present the main research question and sub questions that needs to be answered part of this study, and the scope of the study. Finally, the chapter will explain the thesis key contributions and conclude with providing an outline of the thesis chapters.

1.1 Background of the Study

In a constantly changing and ever-connected threat landscape, staffing cybersecurity positions adequately and efficiently has become one of the most crucial objectives of any business of any size. Certainly, the hallmark of an appropriately staffed, trained, highly competent and proficient cybersecurity organization is ensuring that business operations remain secure, functional and predictable.

Cybersecurity is an integral part of safeguarding information and information systems from alteration, misuse, and unwanted access. The National Initiative for Cybersecurity Careers and Studies (NICCS) (NICCS , 2021) defines cybersecurity as “the activity or process, ability or capability, or state whereby information and communication systems and the information contained therein is protected from and/or defended against damage, unauthorized use or modification, or exploitation.”

There is a constant challenge of protecting information and information systems from cyber-attacks (Evans & Reeder, 2010). Cyber threats have evolved rapidly in recent years and are no longer the domain of a limited number of skilled cybersecurity practitioners. Overall, cybersecurity professionals have to contend with an increasing

velocity of cyber-attacks targeting their infrastructure at a relentless pace. The 2017 Global Information Security Workforce Study (GISWS) (Center for Cyber Safety and Education, 2017) stated that threats of most concern were vulnerabilities, exploits, actors and tactics. Globally, data exposure is recognized to be a top concern for information security professionals, regardless of their geographic location.

According to (Center for Cyber Safety and Education, 2017), it was stated that cybersecurity practitioners, globally, are facing an ever-evolving threat landscape that many feel they are ill-equipped to manage. Additionally, understaffed teams are significantly more likely to have experienced more cyberattacks. In an era of high-profile data exposures and overwhelming cyber-attacks, cybersecurity is deemed to impact every individual and every organization ((ISC)², 2019). Hence, the creation of a cybersecurity industry, educational programs, technical training platforms, policies and strategies that are seamlessly woven in a framework that can address the shortage of skilled cybersecurity resources are deemed crucial.

(ISC, 2020) and (Center for Cyber Safety and Education, 2017) indicate that cybersecurity workforce shortage continues to be a problem for organizations in different industries of all sizes. In fact, the cybersecurity skills shortage remains the number one job concern for those working in the field. However, the skills shortage amongst cybersecurity professionals is a concern that can neither be solved by only the government itself nor by attending more technical training. Resolving a problem of this magnitude requires a comprehensive and holistic multidimensional framework as well as a strategy that will involve educational programs and workforce policy.

The emergence of consumer goods such as wearable devices and autonomous cars, alongside the increasing connectivity of systems managing critical national infrastructures such as power plants and traffic signals, and the introduction of smart cities are all creating new threats to public safety, privacy, and economic stability. These are technological areas that ask for highly proficient, skilled, and technically competent resources to secure and safeguard the ever-evolving technological landscape (Trends & Development, 2019).

Current educational programs and industry specific certifications are not structured to build cybersecurity capacity to meet employers' workforce and skills' demand. First, like any field of study, formal education alone does not necessarily provide turn-key-ready professionals. Second, although some educational institutions are implementing successful technical programs, most are still perceived as training cybersecurity in abstraction, rather than training it as a technical and hands-on field program which, by its very nature, requires some business intelligence (*Training the next generation of cyber warriors . By | Douglas J . Guth, n.d.*).

In addition, the cybersecurity profession did not have any career name, title or a great elaboration of the role and responsibilities that they were required to handle in the organization. Hence, a security specialist will have a different set of responsibilities from one organization to another (NICCS , 2021).

This research study intends to shorten the cybersecurity skills gap and workforce shortage problem by introducing new ways, alongside the current academic cybersecurity program, to upscale the hands-on technical skills amongst students that are graduating from undergraduate computing degrees. Furthermore, this research study intends to

design and develop a cybersecurity skills performance dashboard that aims at providing a true assessment of the cybersecurity professionals' hands-on technical skills in order to understand and measure the true skills gaps that is available and accordingly introduce and create capacity building programs that aim at upscaling the skills that are scarce.

Hence, the ultimate aim of this thesis is a twofold as follows:

1. A thorough experiment and analysis of the effectiveness of the practical methods integrated with the current academic cybersecurity programs to lead the way in shortening the cybersecurity skills gap and workforce shortage problem.
2. Design and development of the cybersecurity skills performance dashboard as a measurement tool to provide factual data on the existent hands-on technical skills.

1.2 Introduction to the Problem

The shortfall of professionals with the required cybersecurity skills set globally has never been more acute. The World Economic Forum (WEF) summed up the plight as “nowhere is the workforce skills gap more pronounced than in cybersecurity”. There are numerous supporting pieces of evidence conducted by renowned scientific research institutions that highlight the cybersecurity skills gap around the globe (i.e., cybersecurity professionals that lack the required technical skills) and skills shortage (i.e., lack of skilled cybersecurity professionals to work in technically specific cybersecurity job roles). Most of the research sources make similar affirming observations in regards to the cybersecurity skills shortage for the last 8 years.

1.2.1 IPSOS MORI Research

IPSOS MORI conducted recent research in 2021 to understand the current UK cybersecurity skills labor market. The researchers observed that a high proportion of UK businesses continue to lack cybersecurity professionals with the appropriate technical skills to manage daily cybersecurity tasks and responsibilities. Approximately 50 percent of UK businesses have a basic technical skills gap and 33 percent of businesses have advanced cybersecurity skills shortage (i.e., areas such as penetration testing, digital forensics and security architecture) (Ipsos MORI, 2021).

1.2.2 EMSI, ESG and ISSA Research

Last year, EMSI released a research report that revealed that the United States has less than half of the cybersecurity professionals it needs to keep up with the high demand of cybersecurity talent (i.e., for every 100 active cyber security jobs posting, there is only a mere 48 qualified cybersecurity talent to fill) (EMSI, 2020). Last year as well, Enterprise Security Group (ESG) and Information Systems Security Association (ISSA) illustrated the past four years statistics where the cybersecurity shortage percentage ranged from a low of 69 percent to a high of 74 percent, pointing at a lack of advancement in bridging the cybersecurity skills gap (ESG Global and ISSA, 2020).

1.2.3 Cybersecurity Ventures Research

In the year 2019, Cybersecurity Ventures reported that there would be a global shortfall of 3.5 million unfilled cyber security jobs by 2021, which is an increase from one million positions that were reported in 2014 (Cybersecurity Ventures, 2019). Another 2019 study, funded by the National Initiative for Cybersecurity Education (NICE), showed that

the US observed a shortage of almost 314,000 cyber security professionals as of Q1 of 2019, and the number of unfilled cybersecurity jobs has grown by more than 50 percent since 2015 (CyberSeek, 2019).

1.2.4 MIT Technology Review

In 2018, an MIT Technology Review research report observed that from the cybersecurity candidates who apply for such jobs, only fewer than one in four are even qualified to fill the job (MIT Technology Review, 2018). (ISC)² also produced a 2018 report of an around the globe research which concluded that the lack of cyber security talent was at nearly 3 million. An alarming increase from a report (ISC)² put out just a year earlier in 2017 stated a radically lower 1.8 million figure by 2022. (ISC2, 2018) Figure 1: Depicts (ISC)² study statistics of cybersecurity skills shortage for the various regions around the world settling at almost 3 million globally.

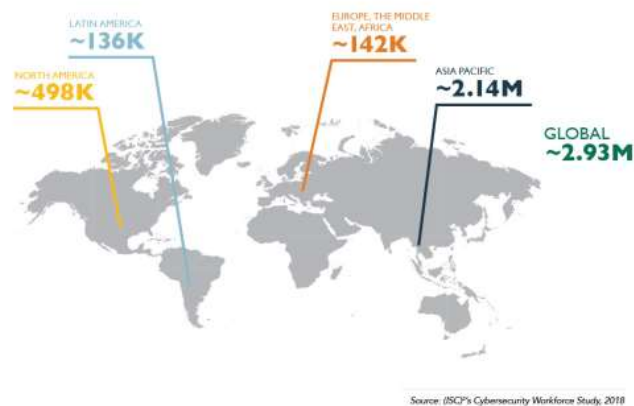


Figure 1: ISC2 2018 Study of Cybersecurity skills shortage around the globe of nearly 3 million professionals

As observed by various studies conducted by numerous research institutions and industries, the cybersecurity skills shortage is a recurring problem, year by year. The previous elaborated research studies show that the problem has been there for the last 8 years and is predicted to continue for years to come. Also, it is a problem that various countries and governments focus on addressing and resolving.

Businesses today are highly reliant on cybersecurity workforce with basic technical skills to fulfill advanced cybersecurity requirements, which is not the key to reach for a high level of security maturity in a given entity nor shall the business be able to fight off hackers when a cyber-attack or breach takes place with unskilled cybersecurity professionals.

In addition, with the continuous evolvement of the cyber threat landscape and the surge of new technologies such as Industry 4.0, IoT, AI/ML, digital transformation, OT security, and smart infrastructure, the shortage shall be seen by businesses as an existential threat rather than a minor inconvenience. As these new technological developments evolve, businesses continue to be in need of advanced technical skills such as programming, analyzing large datasets, managing various networks, etc. If there is one thing to take away, it is that it is time to find a solution that can shorten the skills shortage problem at a time when the demand for cybersecurity practitioners is increasing, yet the supply is stagnant.

1.3 UAE Cybersecurity Educational Programs

There are many educational institutions in the UAE that offer an undergraduate cybersecurity program or a computing degree with a specialization in information or cyber security. In this research work, top-ranked and renowned universities in the United Arab

Emirates were researched to explore their current curricular guidelines for undergraduate cybersecurity education. The course catalog of these universities was studied thoroughly to discover relevant courses offered in those selected universities. The universities that were searched were Abu Dhabi Polytechnic Institute (AD Polytech) and Khalifa University (KU); both of these universities are based in Abu Dhabi. The Higher Colleges of Technologies (HCT) and Zayed University (ZU) are universities that have campuses in all the seven emirates of the UAE.

It has been found that all these universities had the first and second year of study as foundational courses with no courses that offer any hands-on technical courses in the field of cybersecurity. It is in the 3rd and 4th-year of the undergraduate degree program that there is an introduction of foundational building block courses in the field of cybersecurity such as: Networking and Systems, Cryptography, Introduction to Information Security, Digital Forensics, etc. These universities, besides the courses in the field of cybersecurity, also have lab sessions where the students practice basic hands-on technical exercises. The lab session duration is an hour to 2 hours for the student to complete the given exercise.

Finally, it was explored that the delivery model for the coursework throughout the four years was a combination of classroom lectures, assignments, group projects, presentations, lab exercises, quizzes, mid-term exams and a final exam. It was not found in any of the selected universities or any university within the UAE that offered a gamification platform to learn from, or extensive scenarios of simulated real-world environment to execute, nor teaching of any technical skills such as penetration testing, threat hunting, incident response, security monitoring and operations, etc.

This was one of the major reasons that led to working on this research study, to evolve the current undergraduate cybersecurity educational program into one that integrates the technical gamification simulation platform to upscale the hands-on technical skills of the students.

1.4 Capacity Building: UAE Cybersecurity Strategy

According to the UAE Telecommunication and Digital Regulatory Authority (TDRA), the (TDRA, 2020) National Cybersecurity Strategy of the UAE stands on the objective of reducing the impact of cybersecurity incidents ranging from direct financial impact, client impact, and service impact to reputational impact. The strategy leverages global industry reports, cybersecurity experts and 10 leading cybersecurity ecosystem benchmark countries to improve its efficacy and implementation. More specifically, the strategy aspires to build confidence to participate in the digitally cohesive world securely, commemorate contributions to improving cybersecurity, fostering a dominant culture of entrepreneurship, enabling small-to-medium sized enterprises to safeguard themselves against commonplace cyber-attacks, protecting critical information concerning infrastructure assets and building a benchmark cybersecurity workforce (TDRA, 2020).

In an attempt to develop the UAE's cybersecurity ecosystem, the national strategy was set on seven pillars: driving demand, access to financing, culture and mindset, innovation and technology adoption, ease-of-doing-business, business support, and capacity building. The pillars are designed to holistically reach the target of developing capabilities of more than 40,000 cybersecurity professionals.

However, the problem lies in the appropriate methodology in place to identify and measure the upscale in the hands-on technical skills to meet the capacity building pillar

of the UAE cybersecurity strategy. Currently there exists no mechanism in place in regards to factual data in regards to:

1. Number of cybersecurity professionals that exists in the UAE to serve and fill in the active job postings in the field of cybersecurity;
2. Existent technical skills that are available and portrayed in the cybersecurity professionals;
3. Rare technical skills that need to be trained and developed to increase the number of cybersecurity professionals in that area;
4. Country wide technical gamification simulation platform that can be used by students at educational institutions that are majored in cybersecurity;
5. Nation-wide database or repository of the current existent cybersecurity skills performance dashboard for the cybersecurity professionals; and
6. Any statistics or factual data that can be used as a starting benchmark to tailor, create, and introduce a phased-out capacity building program.

Hence, this is yet another problem that was the reason to initiate and work on this research study in order design and develop a cybersecurity skills performance dashboard (CSPD) that can act as a nation-wide repository of factual data in regards to the true assessment of the cybersecurity skills that currently exists and use this data to introduce a well-structured capacity building program to upscale the inexistent technical skills.

1.5 aeCERT and ADDA Cybersecurity Workforce Framework

According to the UAE Computer Emergency Response Team (aeCERT), the UAE National Cybersecurity Workforce Framework (aeCERT, 2021) is designed as the fundamental initiative to guide cyber and information security recruitment, education, and

training & skills development. The primary objective of the framework is to bridge the gap between public and private segments of the cybersecurity workforce as well as create increased cybersecurity awareness to accentuate the workforce requirements. Owing to the critical nature of the UAE cybersecurity landscape and the surging number of cyber incidents, the framework insists on developing a workforce that complies with the organizational requirements, understands the recent cybersecurity risk posture of the organisation, and complies with the applicable laws and regulations related to cybersecurity (aeCERT, 2021).

According to the report by (aeCERT, 2021), the cybersecurity workforce framework is developed by organizations and individuals for instructing a unified approach in developing cybersecurity structures and fostering within and beyond team developments. The framework also focuses on making awareness through the senior management of organizations to better identify the cybersecurity workforce they employ in terms of knowledge, skills and abilities (KSAs). Moreover, the framework signifies improving the competency of the workforce and being capable enough to keep developing their skills with recent technological advances. More holistically, the aeCERT workforce framework focuses on human capital development as much as the effective utilization of cybersecurity professionals across all kinds of domains and industry sectors. The lack of guidance in career development and skill deployment is a crucial concern in the framework (aeCERT, 2021).

Additionally, the Abu Dhabi Digital Authority (ADDA) Cybersecurity Guidelines (ADDA, 2021) focuses on the strategic objective of incorporating robust cybersecurity professionalism and increasing security maturity levels across the Emirate of Abu Dhabi.

The cybersecurity guidelines of ADDA follow through to build the fundamental building blocks for the cybersecurity field from monitoring the workforce skills to guaranteeing their efficacy to optimal allocation. More specifically, the workforce guidelines offer grounds for organizations and private corporations to structure or revise their internal cybersecurity units according to the variance and degree of threat to data integrity and confidentiality (ADDA, 2021).

For the purposes of this research study, the ADDA cybersecurity workforce roles workbook used as the base for deriving the knowledge, skills, and abilities for the various cybersecurity roles for the cybersecurity skills performance dashboard that was designed and developed as a contribution to this research.

1.6 Statement of the Problem

It is apparent that governments around the globe have a great need for technical competence and qualifications to protect and safeguard their national cybersecurity infrastructure besides its public and private sectors. The ISC (2021) study shows a staggering shortage of 3.1 million cybersecurity professionals around the world. The gap is most significant in Asia with a shortage of 2 million individuals, followed by a shortage of 527,000 professionals in Latin America, 376,000 professionals in North America and 168,000 in Europe.

Numerous researches show that currently, there exists not only a cybersecurity skills shortage globally in the cybersecurity labor market but also a deficit in the supply of the number of cybersecurity professionals to fill in the several active technical cybersecurity job postings globally. Therefore, there is a crucial need today to introduce new ways into the academic structure of cybersecurity undergraduate programs that shall

not only shorten the cybersecurity skills gap but also increase the number of cybersecurity professionals to address the deficit in the supply problem as well.

The ever-increasing number of fresh graduates that complete their cybersecurity undergraduate education and that are prepared to enter the cybersecurity labor market undergo the traditional academic cybersecurity program of coursework and minimal technical hands-on exercises. The population targeted via this research study are these undergraduate students who are actively enrolled in cybersecurity undergraduate programs so as to effectively improve their technical hands-on cybersecurity skills.

To add further clarity to the problem in hand, the cybersecurity skills shortage has two main components. The most evident one, through previous research, is that there are not enough cybersecurity professionals to fill the existing cybersecurity active job postings around the world. Hence, the businesses are targeting the exact same experts that are available in the cybersecurity workforce pool. Another component to this shortage is that there is an acute shortage in the number of skilled and proficient cybersecurity professionals that have advanced cybersecurity skills set such as a cyber-threat hunter, reverse engineer, digital forensics investigator, cloud security architect, cyber incident responder, and many more of these unique and advanced cybersecurity skills needed for these job roles.

This research study aims to address the second component of this problem that is the acute shortage of a skilled and proficient cybersecurity taskforce. This research addressed this problem in two unique ways as follows, by:

1. Design and development of a Cybersecurity Skills Performance Dashboard (CSPD) in order to understand and measure the current available hands-on

technical cybersecurity skills to leverage. In addition, to understand the shortage of skills that needs to be targeted to develop and train.

2. Conducting a thorough experiment and analysis to explore and understand the effectiveness of introducing Technical Gamification Simulation Platform integrated with the current academic cybersecurity programs to upscale the hands-on technical skills eventually lead the way in shortening the cybersecurity skills gap.

The reason this research study took this route of designing and developing a skills performance dashboard is to address the major problem of lack of visibility into the current skills gap that exists in the UAE. Although studies and market recruiters show that there is an acute need for cybersecurity skilled professionals in various advanced technical fields. However, there is no such platform or statistics in place that can measure the scale of this cybersecurity skills gap.

As of today, the UAE cybersecurity strategy does mention that they need to develop and train almost 40 thousand cybersecurity professionals. However, as of today there is no evident empirical evidence to how that number has been derived as there is no underlying statistics that can derive what is the appropriate number of cybersecurity professionals needed to fill in the active cybersecurity job postings today and over the coming years.

1.7 Purpose of the Study

The purpose of this study is twofold,

1. To understand and explore how the use of the technical gamification simulation platform (TGSP) will enhance the hands-on technical skills of undergraduate students majored in cybersecurity. This shall be achieved by introducing new ways to teach the academic cybersecurity undergraduate programs that can increase the acquired technical skills set amongst undergraduate students. Qualitative methodological research shall be conducted that includes three phases of 1. Assess, 2. Train, and 3. Perform as the structure of the experiment program to understand and evaluate the effectiveness of introducing the use of technical gamification simulation platform (TGSP), alongside the traditional academic undergraduate cybersecurity program. The goal here is to improve the technical hands-on cybersecurity skillset of this target population to increase the sufficient supply of competent and skilled cybersecurity professionals who are available to fill in the active technical cybersecurity job postings from day one, both in the public and private sector around the globe.
2. To design and develop the cybersecurity skills performance dashboard in order to provide a true assessment of the cybersecurity professional hands-on technical skills. This dashboard shall act the nationwide repository in order to provide factual data on the existent skills and those that need to be developed and trained.

1.8 Scope of the Study

The scope of this study is limited to significantly increasing the supply of skilled and technically proficient cybersecurity professionals in the United Arab Emirates. Since the country already has in place and officially published a cybersecurity strategy, instituted numerous cybersecurity educational programs and has a high industry demand

for cybersecurity expertise. The focus of the skills gap and workforce shortage in this study only applies to the cybersecurity domain.

This research study is limited to cybersecurity participants who pursue their undergraduate degrees within the UAE and are UAE Nationals. All the participants considering both male and female are 3rd or 4th-year students that have either completed all the required university coursework and are left with a summer internship program or have one additional academic year to complete. The participants will have hands-on technical experience on the TGSP during the experiment program that extends over 8-weeks. Over the course of the 8-weeks, there will be close interaction with the students by providing them with access to the TGSP in a controlled environment, and various challenges shall be assigned to them to complete in order to measure if they can complete those assigned challenges successfully. Via an administrative dashboard, their performance will be monitored to know if they have completed the assigned challenges or not. By completing the assigned challenges, the cybersecurity skills performance dashboard will provide a true assessment of the cybersecurity technical skills they have acquired over the period of 8-weeks.

The dashboard shall also indicate the number of times a participant has re-attempted the challenge and the various categories' challenges each participant has completed. Furthermore, the dashboard shall provide a leaderboard ranking that will rank the most skilled cybersecurity participant compared to the rest of the participants.

The number of participants selected for this experiment were a total of 9 participants and all of them were UAE nationals. The reason for such limitation and focus on the nationality is due to the availability of research funding to conduct the experiment.

1.9 Research Objectives and Significance

The objective of this research study is to understand and explore the effectiveness of the use of the technical gamification simulation platform (TGSP) to improve cybersecurity hands-on technical skillset amongst undergraduate students who are majored in computing degrees. In addition to design and development of the cybersecurity skills performance dashboard that will act as a measurement tool to record the hands-on technical skills of the cybersecurity professional and provide factual data on the existent skills and those that are lacking. The two research objectives are aimed to be fulfilled to shorten the cybersecurity skills gap and workforce shortage by producing a superior cluster of undergraduate students who are market ready to fill in the active cybersecurity job postings in the UAE.

There is a need for this research study, as it is first-of-a-kind research, to understand and explore the effectiveness of introducing the use of a technical gamification simulation platform (TGSP) alongside the existing traditional academic cybersecurity undergraduate programs. The TGSP shall be available to be accessed by the students at their convenience wherever they are, whether at home or at the university premises and whenever they want. In short, it is a technical platform that is available to be accessed around the clock. The TGSP is a practical technical hands-on test-bed that provides students with a true simulated real-world environment. Also, it depicts an organization's infrastructure in whichever industrial sector it belongs to by providing them the ability to experiment and execute with a trial-and-error scenario without impeding on the availability of the network or causing chaos to a production environment. In addition, the TGSP will not require students to have an in-person instructor to guide and direct as

it enables a self-efficacy learning capability that shall enable them to continue learning and executing the challenges even after completing their undergraduate programs. Notably, they shall continue to have hands-on experience whilst being a cybersecurity professional.

Moreover, this is a first-of-a-kind research study that designs and develops a skills performance dashboard that shall act as a nationwide repository/database by providing true assessment of the skills that a particular country has and those that needs to be trained and developed. Having such a dashboard is of value for various entities such as government entities, policymakers, private sector, local security authorities, and many more to use these data as benchmark to create and introduce upon it other capacity building programs or benefit from these cybersecurity professionals in their organizational setting.

The main two reasons this research study focused on the undergraduate students' component as the targeted population to address the problem is because:

1. These students have firsthand knowledge about the emerging technologies that transcend their course teachings in the academic institution. Hence, it is easier to build the required technical gamification simulation scenario/challenge in the platform for an IoT or AI/ML or ICS/OT security or big data and so on; and
2. Second, because the majority of the population that increases the supply of the required workforce is that of students that are graduating from several universities within the UAE every semester and are ready to fill in the available

active cybersecurity job postings. Hence, it only makes sense to join forces and work on these fresh minds to build the required technical hands-on skills.

In addition, the importance of this study is that it will act as the first of its kind research results and serve as a benchmark to understand whether there is a need to introduce the use of such a technical simulation platform alongside the academic cybersecurity program in all the universities within a given country and around the globe. Hence, there is a dire need to conduct this research to understand how we can tackle this acute problem of skills gap and workforce shortage challenge to reach a status quo and to introduce new ways to our current cybersecurity academic programs.

Furthermore, there currently exists no comprehensive overarching framework that connects the UAE cybersecurity strategy (TRDA aeCERT, 2019) and policies to the educational system and the UAE cybersecurity industry market. It is, therefore, the aim of this research study to add value and connect the dots by introducing the cybersecurity skills performance dashboard that will connect the three elements i.e., the educational body, with the policy makers and the industry. There are several beneficiaries to the skills performance dashboard as briefly explained as follows:

1. The UAE Cybersecurity Council: this is the highest cybersecurity authority in the UAE and one of its mandates are to understand what is the current status of the cybersecurity skills gap and to develop the required cybersecurity capacity building strategy to bridge this skills gap. Hence, the dashboard shall provide the required empirical evidence to the council on the existing skills and the skills that need to be trained and developed amongst the cybersecurity professionals.

2. The Local Security Authorities: these are the likes of Dubai Digital Authority (DDA), Abu Dhabi Digital Authority (ADDA), and so on. These are local security authorities that are mandated besides their other cybersecurity responsibilities, to ensure there are effective capacity building programs to upscale the required hands-on technical cybersecurity skills basic and advanced for the cybersecurity professionals. Furthermore, these local security authorities are always on the search for superior skilled and talented cybersecurity professionals who can join their team. Hence, this dashboard is instrumental to these authorities as it shall provide the needed factual information on their mandates and requirements.
3. Academic Institutions and Professional Training Institutes: both of these entities are interested to understand how can they plan and prepare their academic curriculums and training programs in order to upscale the hands-on technical skills of their students and cybersecurity professionals in order to meet the needs of the cybersecurity market in the UAE.
4. Public and Private Sector: are also considered beneficiaries of the dashboard as they are always on the lookout on the available skilled and talented cybersecurity professionals that exists by accessing the information in the dashboard. Hence, cutting down on the time to search for the needed talent. The public and private sector in here refer to those in the UAE and worldwide.
5. Cybersecurity Professionals: are also beneficiaries of the dashboard as they can use the dashboard to follow on their progress with the training programs that they have undertaken and the skills that they have gained over time. It can act as a

credible source for them to portray their skills and talent for their prospect employers.

Chapter 5 which is about the design and development of the cybersecurity skills performance dashboard section 5.2.1 explains thoroughly about the beneficiaries and stakeholders of the skills performance dashboard.

1.10 Research Questions

The current absence and negligence of home-grown innovative cybersecurity initiatives have led to an increase in the skills gap and the lack of supply of proficient cybersecurity professionals to cater to the business needs of various business entities. Thus, the increase in the skills gap and workforce shortage in the long term will only lead to businesses' ICT environment being inadequately protected against the vast range of cyber threats and evolving cyber-attacks. Hence, it is deemed crucial the need to have a sufficient supply and availability of a superior cluster of cybersecurity practitioners who can better protect businesses, governments, agencies, and the industry sector as a whole. Policy makers need to be informed on well-researched and practical approaches that can be implemented in order to address the ever-growing skills gap and workforce shortage problem.

The central research questions this study intend to provide a factual answer to is:

Can the use of the technical gamification simulation platform (TGSP) upscale the hands-on technical skills amongst cybersecurity undergraduate students?

The following are the research sub questions to understand and explore during this study:

- **RQ1:** *What are the students' hands-on technical skills experiences once they complete their 4th-year cybersecurity undergraduate degree program?*
- **RQ2:** *What are the students' hands-on technical skills experiences once they complete the cyber range gamification platform scenarios (i.e., both Battle Rooms and Missions)?*
- **RQ3:** *What are the students' hands-on technical skills experiences once they complete the capture the flag gamification platform scenarios?*
- **RQ4:** *What are the student's experiences on the effective training platform considering the cyber range and/or capture the flag?*
- **RQ5:** *How can the hands-on technical skills acquired by the students using the technical gamification simulation platform can be validated using the dashboard?*

1.11 Assumptions and Threats to Validity

Assumptions made in this research study were the following:

1. The study partially depends on surveying participants, sending out questionnaires and conducting one-on-one interviews. Hence, the first assumption is that the respondents of the survey and/or the interviews shall provide honest, legitimate and reliable data towards the research. Careful consideration shall be made when developing these surveys and questionnaires to ensure that it does not conflict with non-disclosure agreements (NDAs) that cybersecurity professionals are obliged to.

2. The next assumption is that the chosen research method for this study to help gather data from the participants through surveys, questionnaires, and interviews will aid access to the current level of technical skillset that participants have before having access to the TGSP. Afterwards, a post-experiment questionnaire shall be rolled out after the participant's experience using the TGSP. This collected data shall assist in identifying the challenges that exist in the current traditional academic undergraduate cybersecurity programs, help develop an improved addition to the academic program and improve the cybersecurity capabilities amongst the students.

Besides the above listed assumptions, there exist few threats to validity. *First threats to validity point* to this research is the similarity of cybersecurity profession that the researcher of this study shares with the participants of this research, and this research will keep aside any bias or influence that have been accumulated over the course of 20+ years in cybersecurity career experience. *Second threats to validity point* to this research is the scarcity of academic literature and research papers entailing the skills gap and the workforce developments in relation to the state of cybersecurity. However, the cybersecurity research institutions and the cybersecurity industry market globally have published a plethora of research studies and reports that tackle this problem. Hence, it has been crucial to approach non-academic papers to inform this research study in terms of how acute the skills gap problem is and how deficient the supply of cybersecurity practitioners across the globe is.

The cybersecurity research institutions that the data is drawn from are the likes of the National Institute of Standards and Technology (NIST), the National Initiative for

Cybersecurity Education (NICE), the Workforce Framework for Cybersecurity, the National Initiative of Cybersecurity Careers and Studies (NICCS), the International Information Systems Security Certificate Consortium (ISC)², including other government and cybersecurity research reports on this matter. *Third threats to validity point* to this research is that the data gathered from the participants will have a different weight on the overall results and this is depending on the universities that they gain academic instruction from, their passion towards choosing cybersecurity as a career, and so on. The data derived from these various different sets of participants will enrich the accumulated data and open opportunities for future research. *Final threats to validity point to this research* is that the scope of this research study is limited to cybersecurity participants who pursue their undergraduate degrees within the UAE and are UAE Nationals. Furthermore, all the participants considering, both male and female, are senior year (i.e., 4th year) students that have completed all the required university coursework and are left with a summer internship program. The participants will have hands-on experience of the TGSP in the provided summer internship period that extends over an 8-week duration period.

1.12 Thesis Key Contributions

The core of this research study is interdisciplinary as it intends to bridge the gap between cybersecurity education at universities and the real-world technical hands-on industry challenges. As well as present a dashboard that can provide the required visibility to measure the scale of the skills gap that currently exists in the UAE and based on this dashboard informed decisions can be taken in order to introduce the needed capacity building campaigns to upscale the needed hands-on technical skills in the UAE.

The key contributions of this thesis are as follows:

1. First and foremost, this research work contributes directly to the literature and the body of knowledge in the following areas:
 - a. First, adding literature to the area of cybersecurity education. This is done by introducing new ways that shall enable universities to produce a superior cluster of cybersecurity workforce that are capable of protecting the businesses as soon as they graduate.
 - b. Second, adding literature in the area of strategy and public policy. This is fulfilled by providing the required guidance to the appropriate authoritative entities to introduce skills performance dashboard as a measurement tool to provide the required visibility of the scale of skills gap that exists and how the insight gained from the dashboard can be leveraged to shorten the skills shortage gap.
2. Secondly, this research work provides the design and development of a cybersecurity skills performance dashboard (CSPD). This dashboard is beneficial in a variety of ways as follows:
 - a. It can act as a nation-wide cybersecurity skills performance dashboard to provide a true assessment of a cybersecurity professional's skills, abilities, and knowledge (KSAs) that can eventually inform businesses of the talents needed for their cybersecurity needs.
 - b. Moreover, the dashboard can act as an invaluable tool that shall inform the policy makers and the strategic authorities of the skills widely available and

the skillset that needs to be developed through the introduction of various cybersecurity home-grown initiatives.

- c. Furthermore, the dashboard provides the cybersecurity professionals the required insights into the skills that they currently have as well as the skills that they are willing to develop in future.
 - d. In addition, the dashboard can act as a credible platform for businesses to validate the skills of the cybersecurity professionals.
 - e. Finally, and most importantly, the dashboard shall provide the needed visibility and insight on the scale of the skills gap that exists in the UAE and how the concerned beneficiaries can leverage this information to introduce the needed capacity building programs, such as
 - i. Better planning of academic programs; and
 - ii. Better alignment with professional training institutions to introduce the needed programs over the period of time.
3. Thirdly, although this dashboard is designed and developed for the purpose of measuring the scale of cybersecurity skills gap, however, this platform can be generalized and applied to any other field of expertise to have empirical evidence about the skills that are available and those that are infrequent.
4. Fourthly, the beneficiaries of the dashboard is not limited to the United Arab Emirates. All other entities worldwide shall be able to access and benefit from the information displayed on the dashboard.
5. Finally, this research work provides a thorough experiment analysis to understand and explore how the use of the technical gamification simulation platform (TGSP)

enhances the hands-on technical skills of undergraduate students majored in cybersecurity. This introduces new ways to teach the academic cybersecurity undergraduate programs that can increase the acquired technical skills set amongst undergraduate students and create market ready cybersecurity professionals to fill in active cybersecurity job postings as soon as they graduate.

1.13 Chapter Summary

This chapter presented the introduction and background of the research work, along with research aims and objectives. It also stated the problem that needs to be tackled and its significance to the UAE environment. The chapter also presented the research question that needs to be answered, and the scope of the study. Finally, the chapter presented the thesis key contributions and concluded with providing an outline of the thesis chapters. In the next chapter, both the literature review and the theoretical / conceptual framework shall be presented.

1.14 Outline of the Thesis Chapters

The research aims and objectives were achieved and discussed elaborately within the context of the thesis chapters. Table 1.1 below provides an outline of the thesis chapters and a summarized description of each chapter.

Chapter	Title	Summary
Chapter 1	Introduction	This chapter provides a review of the background on cybersecurity skills gap and workforce shortage issue. It also interpolates the problem statement and its significance, and the purpose of the study. Furthermore, it states the research objective, research question and sub questions, the scope of the study, and research assumptions & threats to validity. Finally, the chapter presents

the thesis key contributions and provides an outline of the thesis chapters.

Chapter 2	Literature Review	This chapter deeply explores the relevant topics such as current cybersecurity threat landscape, recent cyber-attacks, and the impact of COVID19, cyber threat statistics, cybersecurity landscape in the UAE, and cybersecurity skills and workforce shortage. The chapter also provides a review of the literature related to the topic under study and identifies any gap that might exist in the literature. Finally, the conceptual framework is proposed.
Chapter 3	Research Methodology	This chapter illustrates the methodology used in this research work and elaborates on various topics such as the research design & approach, method applied, target population & sample size description, data collection process, research setting, instruments, data analysis, and data presentation. It also presents the ethical considerations and validity & reliability of the data.
Chapter 4	Results and Discussions	This chapter examines the results generated through the use of technical gamification simulation platform experiment and shall allow the testing of the stated research questions. The chapter will also present a thorough discussion of the major findings based on the data collected to approve or deny the set research questions
Chapter 5	Design and Development of Cybersecurity Skills Performance Dashboard	This chapter describes the approach followed to design and develop the cybersecurity skills performance dashboard. This chapter also elaborates on the various dashboard views to present the cybersecurity professional skills, and maps it to the appropriate role to fill. The chapter concludes with presenting the validation of the design and development of the dashboard.

Chapter 6	Conclusion, Findings and Recommendations	This chapter presents the conclusion of the research work conducted and recommendations along with the research threats to validity, and direction for future works.
-----------	--	--

Table 1: Outline of the Thesis Chapters

Chapter 2: LITERATURE REVIEW

Cybersecurity practitioners agree that the security of any organization depends equally on both the superiority of the technical skills of an organization's security team and technical controls and countermeasures that an organization employs. Recent research studies of the cybersecurity threat landscape indicate that every segment of an industry is susceptible to cyber-attacks and the government's critical infrastructure sector tops the list for targeted security incidents (Benson, McAlaney, & Frumkin, 2019). At the present day, organizations cannot continue to use the traditional cybersecurity approach of safeguarding their information and information systems against unknown threats as this old school approach of cybersecurity protection cannot withstand the rate at which technologies, threats, and vulnerabilities are surfacing.

Cyber threats introduced and used by cyber adversaries have evolved rapidly in recent years and are no longer the domain of a limited number of skilled cybersecurity practitioners. Consequently, there exists a surging demand for cybersecurity practitioners to continuously hone their technical skills and keep up with an ever-evolving cyber threat landscape. Furthermore, educational cybersecurity programs need to constantly evolve to ensure they produce a market-ready superior cluster of cybersecurity professionals who can robustly protect organizations whenever they join.

The present-day reliance on information systems, emerging technologies, and complex networks cannot be overemphasized. Today, the world is rapidly embracing digitalization, which, despite its overwhelming benefits, signifies the need to strengthen cybersecurity practices. The emphasis on cybersecurity has tremendously increased due to the rise in the number of cybersecurity attacks, vulnerabilities, and threats targeting

private corporations, government entities and intelligence agencies. Hence, an increased level of cybersecurity controls and countermeasures is required within and beyond businesses. While cybersecurity workforce training and development has received widespread attention in the previous decade, significant gaps between the availability and high demand of cybersecurity practitioners continue to exist (Ipsos MORI, 2021). The cybersecurity skills gaps are further worsened by the constant shifting nature of cybersecurity threats and attacks, thereby making it crucial to further enhance and introduce new effective initiatives of cybersecurity workforce training and development practices.

In this chapter, the review of literature shall begin by presenting an understanding of the definition of cybersecurity and its core elements to build the foundational knowledge. Next, it will elaborate on the rapidly evolving cyber threat landscape, and cybersecurity attacks and statistics shall be assessed as well. Along with that, the literature review shall elaborate on the impact of the COVID19 pandemic, the surging demand for cybersecurity skills, the significance of staffing cybersecurity professionals and the effect of shortage of cybersecurity expertise. Further, a detailed exploration of the cyber threat landscape in the United Arab Emirates, the UAE national cybersecurity strategy, workforce framework, and the increasing need for capable cybersecurity professionals will be presented. Moreover, the literature shall provide insight into the cybersecurity skills gap problem and the approaches that have been explored by current research efforts to shorten the skills gap problem. Before concluding, the review shall identify the research gaps, threats to validity, and conclude the chapter by presenting the theoretical or conceptual framework for this research study.

2.1 Understanding Cybersecurity

Over the recent years, the alarming surge in cybersecurity incidents across public and private sector organizations has contributed to the critical integration of security functions within the structure of organizations. Furthermore, new technological advancement and the increasing need for cybersecurity awareness across various industrial segments have shown the importance of employing cybersecurity protection controls and countermeasures. Hence, the ultimate goal of any organization has been to ensure that the appropriate cybersecurity controls and security teams are in place to minimize the occurrence of a cyber-attack. This section shall explore the broad and specific definitions of cybersecurity along with summarizing the core elements for sustaining cybersecurity at any given entity.

Cybersecurity is an integral part of safeguarding information and information systems from alteration, misuse, and unwanted access. The National Initiative for Cybersecurity Careers and Studies (NICCS) (NICCS, 2021) defines cybersecurity as “the activity or process, ability or capability, or state whereby information and communication systems and the information contained therein is protected from and defended against damage, unauthorized use or modification, or exploitation.” NICCS is the implementation arm of the National Initiative for Cybersecurity Educations (NICE) while NICE is the entity responsible for cybersecurity education and cybersecurity workforce.

Cybersecurity plays a significant role in protecting people and organizations that use the Internet in their everyday life. (Jain & Pal, 2017) Defined cybersecurity as a combination of policies and practices to safeguard information, information systems and networks from unauthorized access. The main purpose of cybersecurity is to mitigate the

occurrence of cyber-attacks, hence, safeguarding the unwanted access to information systems and maintaining the integrity, confidentiality, and availability of organizational assets (Jain & Pal, 2017). The implementation of cybersecurity controls aims at safeguarding organizational crown jewels from attack, disruption, and any other form of cyber threats. These security controls are applied to computers, networks, related hardware, and software to protect information from misuse and manipulation.

According to recent literature, cybersecurity is considered a cornerstone for any organization to protect its information, information systems, and organizational assets from both internal and external cyber adversaries. Although the definition of cybersecurity varies across different disciplines, it predominantly serves the concept of information and information systems' protection and the mitigation of cyber-attacks and threats.

2.2 Fundamental Elements of Cybersecurity

Various research studies highlight diverse elements of cybersecurity that necessitated the implementation of the required protection of cyberspace. This section elaborates on the fundamental elements of cybersecurity.

According to (Jain & Pal, 2017), the focus of cybersecurity on securing the application follows procedural methods to protect applications from malicious threats and attacks that may come through faults in application design, development and maintenance. The sound security of an application is defined as the key to cyber protection from unauthorized access. (Jain & Pal, 2017) Summarize the use of cybersecurity elements in information security with the core purpose of sustaining confidentiality, integrity and availability of private and sensitive information. The same study expands on the use of cybersecurity to mitigate security breaches in email

gateways, websites, wireless networks, and mobile devices. Also, it extends to blocking incoming attacks on emails to configuring connections and keeping network traffic private.

2.3 Cybersecurity threat Landscape

The advent of computer and internet technology encourages the proliferation of numerous cyber threats, mostly widespread and catastrophic (Lou & Tellabi, 2020). Therefore, at the height of global digital transformation lies the vulnerability of Internet users to attacks by adversaries and malicious groups with notorious intentions. An inadequately protected cyberspace exposes massive and critical data to unauthorized access by cyber attackers. Consequently, there is the need to train and develop cybersecurity practitioners that will safeguard the Internet and connected information systems. Most modern technologies aim at digitizing all aspects of human existence (BIPSS, 2012). Interaction with people, collaboration, purchase of goods and services, and work-life balance has been successfully integrated into the Internet (Furfaro, Pace, & Parise, 2020). Today, most companies offer a comprehensive range of digital products and services, which generates a considerable amount of data, often stored in servers (Vigano, Loi, Yaghmaei, Christen, & Gordjin, 2020). Since data has become the core element of modern technological growth, access to massive data is paramount to building digital power. However, the greater our dependence on the Internet, the higher the risk of exposure to cyber-attacks. Cyber threats have matured to become a global issue that every business, government, agency, and practitioner should be wary of because of their parasitic nature (Shires, Cyber-noir: Cybersecurity and popular culture, 2020). Cyber threats can take various forms, including malware, phishing, ransomware, distributed denial of service (DDoS), data breach, data manipulation, identity theft and spoofing

(Gaus, 2013) (Valuch, Gabris, & Hamulak, 2017). Modern-day cyber-attacks do not only aim to breach security protocols as a test of technological competence but to critically disrupt the flow of data (Al-Mhiqani, et al., 2020). Such disruptions can range from system crashes to loss of critical data.

Monitoring the ongoing threats posed by cyber attackers, recent studies indicate that cyber-attacks that target multinational corporations and government organizations can cause substantial damages, especially to its crown jewels (Ionescu, Dumitru, Pricop, & Pircalabu, 2020). Over the years, cyber threats have taken different dimensions, and they include the development of computer viruses, worms, and botnets, the building of advanced and automated phishing and spamming scams. Thus, there is a critical concern for future cyber practitioners (Vidal, Vidal, Monge, & Monterrubio, 2020). The prospective cybersecurity practitioner must be vigilant and constructive in thinking of different defense mechanisms against the evolving cyber threats (Ionescu, Dumitru, Pricop, & Pircalabu, 2020). This is because the greater the invention of hypertensive technologies, the higher the risk of exposure and the greater the attack surface. Hence, cybersecurity practitioners and businesses protecting their big data need to be cautious. From an investigative point of view, it is obvious that cybercriminals take advantage of the volatile and expansive Internet resources to gain unauthorized access to information systems and their resources (Archibald, 2020).

Nevertheless, most of the gaps, which cybercriminals maximize on to exploit web resources, can be attributed to the insignificant mistakes of the system administrators. A certain loophole in a digital program can provide sufficient opportunity for catastrophic invasions (Khera, 2018). Many cyber-attacks in history have been known to cost the

victims both money and reputation in trying to repair the damages and regain the public's trust. The proficient skills of cybersecurity practitioners are often tested by the robustness and resiliency of the technology they build (El-Rewini, Sadatsharan, Selvaraj, Plathottam, & Ranganathan, 2020). Therefore, whether it is a small application for data processing and business transactions or large systems that are processing billions of data per second, strengthening a web resource's security is essential and should remain a top priority in the digital program design, development, execution, and maintenance (O'Connell, 2012).

The protection of cyberspace should further be a focal point for businesses and agencies in this competitive digital age (Vijayakumaran, Muthusenthil, & Manickavasagam, 2020). Therefore, attack-immune online cyberspace demands series of robust layers of security controls or what is known as defense in depth. In essence, cybersecurity practitioners are tasked with ensuring the provision of resilient controls against unwarranted accesses. Moreover, one recommended step in protecting cyber resources may involve the limited and restricted unnecessary users' access to various websites such as installing software and adjusting system settings (Danidou, 2020). Nevertheless, a decreased user permission to online resources amounts to technological inflexibility, user inconvenience, and counteraction of digital personalization which is in contradiction of the aims of recent innovations in technologies. At such a crossroad, the society must prioritize the training and development of cybersecurity professionals and reskilling of existing professionals based on current trends of cyber-attacks (Brilingaitė, Bukauskas, & Juozapavičius, 2020). Thus, an expert cybersecurity practitioner should understand the psychology of cyber-attackers as a prerequisite for implementing the

required cybersecurity controls and countermeasures. Controls such as complex programming, regular checks and maintenance are vital, but an automated and artificially intelligent cybersecurity practitioner is required to face the current challenges (Petit & Shladover, 2015).

(Abu-Taieh, Faries, AlOtaibi, & Aldehim, 2018) affirm in recent literature that the cyber threat landscape is evolving at a near to exponentially growing rate, harnessing the exposure to persistently complex and malicious cyber threats. Hence, the cyber threat landscape spans mitigating cyber-criminal risks and making thorough and well-informed decisions. Due to the continuous evolution of technological advances yielding to the interconnected infrastructure of the world, the cyber threat landscape evolution is inevitable (Abu, Selamat, Ariffin, & Yusof, 2018). Additionally, (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018) have emphasized the ever-increasing digitalization of business operations alongside the lack of effective security metrics and frameworks to comprehend the severity of the potential cyber threats in nature.

2.4 Recent Cyber Attacks

In this section various recent cyber-attacks shall be discussed thoroughly. These attacks tackled are data breaches, ransomwares, and supply chain attacks.

2.4.1 Data Breaches

Cybercriminals typically capitalize on the weakness of technology to attack, which can either be in form of stealing critical information or initiating a dangerous disruption (Morales, 2009). In 2020, data breaches exposed a total of 36 billion records (Sobers, 2021). Historically, even the large corporations with robust cybersecurity defenses have

been subject to cyber-attacks. Yahoo was breached twice in 2013 and 2016, where the attack affected around 3 billion accounts (Pearlso, Saunders, & Galletta, 2019) (Ozkaya & Aslaner, 2019). The attack on Equifax compromised 150 million accounts (Bagley, 2018). Marriott Group was also breached twice with data of 383 million customers, 8 million credit cards and 5 million passports being compromised (Alfred, 2019) (Valinsky, 2020). The world's leading cybersecurity firms are not safe either and can be breached as evident from the recent attack of FireEye (Constantin, 2020).

In 2019, hackers utilized the opportunity of the evolving digital metamorphosis as sweet spots for grounding industries and agencies (Mohasseb, Aziz, Jung, & Lee, 2019). One of the single largest breached personal credentials was the "Collection #1" in which over 700 million email data including 21 million passwords were exposed in a popular hacking forum after being hosted in the cloud. It was a mere precursor of a more devastating 1 terabyte of a data leak that was distributed across the internet (Hunt, 2019). In 2019, The Hacker News reported theft of 620 million account details from 16 hacked websites later auctioned in Dream Market for sale (Khandelwal, 2019). Verifications.io was also victimized with a loss of over 800 sensitive emails containing sensitive information (Diachenko, 2019). About one year ago, Fxmsp, a Russian hacking group, claimed to have penetrated McAfee, Symantec, and Trend Micro Antivirus networks (Arghire, 2019). The invasions of these firms enabled the hackers to obtain undue remote access to their servers. They also stole over 30 terabytes of data, which were later sold to the public.

The banking sector faces daily threats from internet fraudsters (BBC, 2019). Capital One was finally run aground in 2019 after over four years of deliberate attacks on

the financial institution. The data breach exposed the personal information of 100 million credit cards' users (The Washington Post, 2020). To be able to hack the company's systems, the intruders expertly misconfigured a firewall in their servers, thereby altering the design architecture and stealing more than 700 folders containing terabytes of data. Since then, numerous US institutions have been badly affected by cyber-attacks targeted at intercepting data flow, breaching of services or misconfiguration of programs to disrupt the normal performance of servers and databases (Damico, 2009).

2.4.2 Ransomwares

The damage caused by ransomware and malware is on the rise; the average ransomware payment increased by 33% to \$111,605 in 2020 (Sobers, 2021). Studies show that more than 94% of malware is delivered via email (Fruhlinger, 2020). The attackers frequently target important service organizations to instigate a sense of urgency in meeting the demands. For instance, the healthcare industry lost \$25 billion to ransomware attacks in 2019 alone (Sobers, 2021). A major cyber-attack on Lake City's Florida computers resulted in the loss of massive amounts of data as highly reactive ransomwares were responsible for crippling the city's computer systems for over 368 hours (Villas-Boas, 2019).

Another ransomware attack that occurred in 2017 affected the UK's National Health Service, which resulted in the loss of both life and money (Graham, 2017). Another attack in 2015 disrupted the power of 230,000 Ukrainians for over 6 hours (Polityuk, Vukmanovic, & Jewkes, 2017). Similarly, a cyber-attack launched against Turkey resulted in a power outage for over 40 million people (Smart Energy International, 2015). The city of Johannesburg also suffered the same damages as Lake City on 7th July 2017 after a

ransomware attack prevented prepaid electricity consumers from purchasing electricity units from the City Power's electricity website thereby causing a long-term blackout.

2.4.3 Supply Chain Attacks

Cyberattacks can also be initiated via the less-secure supply chain elements (Carnovale & Yenyurt, 2021). In 2017, the shipping giant, Maersk's global activities suddenly came to a standstill when a cyberattack was launched via the accounting software the firm was using in Ukraine (Greenberg, 2018). In the same year, the US Department of Homeland Security directed the federal agencies to discontinue using the Russian Kaspersky products in a somewhat controversial decision (Office of the Press Secretary, 2017). The quantum of supply chain attacks is further on the rise (Arghire, 2019), and Varonis reports that these attacks increased by 78% in 2019 (Sobers, 2021). The recent breach of SolarWinds software shows how devastating the impact can be as the software is used by some 18,000 organizations with the potential of costing billions in remedial action (Korolov, 2021).

2.5 The Impact of COVID-19

The impact of COVID-19 has been felt in almost every industry segment and cyberspace is no exception. The pandemic has opened new opportunities for cybercriminals to exploit vulnerable industries, such as the healthcare industry and the remote workers, to name a few. The FBI reported a 300% increase in cybercrimes since the onslaught of the pandemic (Walter, 2020), with a 238% increase in attacks on financial institutions and a 58% increase in attacks on the healthcare industry in 2020 (Sobers, 2021). In April 2020, Google blocked some 18 million malware and phishing emails

related to the topic of Coronavirus (Kumaran & Lugani, 2020). In the same month, half a million Zoom accounts were compromised and put for sale on the dark web (Ikeda, 2020). The Pandemic Unemployment Assistance Program was used as a window of a data breach attack affecting 33,000 applicants (Collier, 2020).

Precisely, COVID-19 acted as a catalyst in increasing the pace of cyber-attacks. While the increase can be attributed to the distraction caused by the pandemic, the primary factors driving this change include greater usage of home networks, Coronavirus-specific emails and lack of cybersecurity training to engage in remote work. Most cybersecurity functions concentrate on improving organization-wide networks with little attention to covering or securing home networks used by the employees, especially before the pandemic.

2.6 Cyberthreat Statistics

Cyber threat refers to possible malicious attempts performed to damage or disrupt a computer network or system (Imran, Arif, & Shoab, 2018). Studies reveal that the number of cyber threat-related incidents have been increasing in the previous decade, especially during the past few years. (Verizon, 2018) report revealed 5,300 incidents and 2,216 confirmed breaches in 2018, which was an extreme increase from 1,209 breaches reported in 2016. Similarly, a total of 1.1 billion identities were exposed in 2016, which was twice the number of identities exposed in 2015 (Imran, Arif, & Shoab, 2018). In 2018, each attack exposed more than 927,000 identities, and a total of 15 breaches involved the exposure of more than 10 million identities per breach (Symantec Security Center, 2021). The number also rose higher in the subsequent 2 years. In 2020, the number of incidents was as high as 29,206 with 5,275 confirmed breaches (Verizon, 2021). More

than 85% of the breaches involved a human element, and more than 61% involved credentials (Verizon, 2021). A total of 36 billion records were exposed only during the first half of 2020 (RiskBased Security, 2020). The worldwide information security market is forecasted to exceed \$170 billion by 2022, which signifies the importance of protecting sensitive information for businesses as well as users (Sobers, 2021). Despite substantial expenditure, only 5% of the companies' folders and data are adequately protected, which explains how significant the skills gap is. Statistics further reveal that cyber-attacks occur long before they are detected, which further complicates the management process. For instance, the average time to identify a breach is 206 days, and the average time to contain it being 73 days (Oosthoek & Doerr, 2020). Consequently, the cybersecurity domain as well as the magnitude and range of cyber threats are deteriorating rather than improving.

2.7 Cyberthreat Landscape in the UAE

According to the Cyber Resilience Report penned by (Digital14, 2021), UAE is recognized as the second most targeted state for cybercrimes with a subsequent increase in annual losses due to the consequences of cyber-attacks. The high degree of cybercrime losses is summarized to resonate with the impact of a threat to the cybersecurity landscape in terms of financially driven activities. Moreover, the report particularly signifies that the nation-cyber-threat-actors have become significantly active in advancing their interests through further sophistication and detail in their designs. Specifically, the identified motive in the report behind the cyber-attacks is economic and political motivations. Hence, the studies summarize not only the activeness and sophistication of the cyber-crimes but also the complexity of the cyber-crimes that creates

a barrier in identifying the sources. The report provides empirical evidence that the Head of cybersecurity of UAE identified a 250 percent increase in the growth of cyber-attacks across UAE, specifically summarizing the surging rate of phishing and ransomware attacks (Popkova & Gulzat, 2019). According to the report, the attacks are not restricted to stealing and manipulating the data of individuals, but rather follows a widespread motive behind it. The report quotes a study that recognized a 33 percent increase in ransomware attacks from 2019 to 2020. Similar growth was observed in the number of ransomware attacks by 40 percent in 2020.

2.8 UAE National Cybersecurity Strategy

According to the UAE Telecommunication and Digital Regulatory Authority (TDRA), the (TDRA, 2020) National Cybersecurity Strategy of the UAE stands on the objective of reducing the impact of cybersecurity incidents ranging from direct financial impact, client impact, and service impact to reputational impact. The strategy leverages global industry reports, cybersecurity experts and 10 leading cybersecurity ecosystem benchmark countries to improve its efficacy and implementation. More specifically, the strategy aspires to build confidence to participate in the digitally cohesive world securely, commemorate contributions to improving cybersecurity, fostering a dominant culture of entrepreneurship, enabling small-to-medium sized enterprises to safeguard themselves against commonplace cyber-attacks, protecting critical information concerning infrastructure assets and building a benchmark cybersecurity workforce (TDRA, 2020).

In an attempt to develop the UAE's cybersecurity ecosystem, the national strategy was set on seven pillars: driving demand, access to financing, culture and mindset, innovation and technology adoption, ease-of-doing-business, business support, and

education and skills development. The pillars are designed to holistically reach the target of developing capabilities of more than 40,000 cybersecurity professionals. The strategy also plans to create cybersecurity citizen awareness across the states targeting various segments from children, students, professionals, and senior citizens. To further enhance the cybersecurity ecosystem, the national strategy is set to reward excellence in awareness, skill enhancement, entrepreneurship and growth concerning cybersecurity with excellence through the national awards program. Additionally, the National Cyber Incident Response Plan is reportedly devised to enable a smooth, effective, and coordinated responsiveness to cyber incidents and establish a standardized severity assessment matrix to mobilize the required support within time to reduce the impact. The core initiatives for the Cyber Incident Response Plan include establishing a single point of contact, construing advisories for protection against cyber threats, launching active monitoring of cyber threats and regulating the incident reports under cross-agency intelligence sharing (Mavroeidis & Bromander, 2017). For efficacy, the strategy plans to form associations within government institutions, private corporations, academic professionals, and international consortiums (TDRA, 2020).

2.9 UAE Cybersecurity Workforce Framework

According to the UAE Computer Emergency Response Team (aeCERT), the UAE National Cybersecurity Workforce Framework (aeCERT, 2021) is designed as the fundamental initiative to guide cyber and information security recruitment, education, and training & skills development. The primary objective of the framework is to bridge the gap between public and private segments of the cybersecurity workforce as well as create increased cybersecurity awareness to accentuate the workforce requirements. Owing to

the critical nature of the UAE cybersecurity landscape and the surging number of cyber incidents, the framework insists on developing a workforce that complies with the organizational requirements, understands the recent cybersecurity risk posture of the organisation, and complies with the applicable laws and regulations related to cybersecurity (aeCERT, 2021).

According to the report by (aeCERT, 2021), the cybersecurity workforce framework is developed by organizations and individuals for instructing a unified approach in developing cybersecurity structures and fostering within and beyond team developments. The framework also focuses on making awareness through the senior management of organizations to better identify the cybersecurity workforce they employ in terms of knowledge, skills and abilities (KSAs). Moreover, the framework signifies improving the competency of the workforce and being capable enough to keep developing their skills with recent technological advances. More holistically, the aeCERT workforce framework focuses on human capital development as much as the effective utilization of cybersecurity professionals across all kinds of domains and industry sectors. The lack of guidance in career development and skill deployment is a crucial concern in the framework (aeCERT, 2021).

Additionally, the Abu Dhabi Digital Authority (ADDA) Cybersecurity Guidelines (ADDA, 2021) focuses on the strategic objective of incorporating robust cybersecurity professionalism and increasing security maturity levels across the Emirate of Abu Dhabi. The cybersecurity guidelines of ADDA follow through to build the fundamental building blocks for the cybersecurity field from monitoring the workforce skills to guaranteeing their efficacy to optimal allocation. The awareness campaigns range from high school students

to guaranteeing the interest amongst graduates for pursuing their careers in cybersecurity. The long-range plan reports to be holistic in stressing responsiveness and coordinated cybersecurity workforce. More specifically, the workforce guidelines offer grounds for organizations and private corporations to structure or revise their internal cybersecurity units according to the variance and degree of threat to data integrity and confidentiality (ADDA, 2021).

2.10 UAE Cybersecurity Landscape Review

While the literature and the UAE National Cybersecurity Landscape signifies the dynamic nature of the cybersecurity threats across the UAE along with difficulty in determining and remediating them, the Response Plan and National Strategy seems to be holistic in addressing fundamental to critical concerns. The National Strategy, the Cyber Incident Response Plan and the Workforce Frameworks designed by (aeCERT, 2021) and (ADDA, 2021) seem to be effective if deployed in a structured and efficient way. The strategies comprehensively cover the aspects of cyber awareness, skills development and deployment of cybersecurity professionals. Along with the workforce development, the guidelines focus on organizations in addressing the requirements for consistent investment in the workforce to deal with the increasing complexity of the future cyber threat landscape. Additionally, the strategy, the framework, the plan and the guidelines identify the related adversaries for further effective implementation. However, despite the holistic nature of the national strategy and response plan, the UAE cybersecurity framework fails to centralize the management to oversee, supervise and hold accountable the affiliations and the adversaries involved. Knowing the crucial spectrum of risks involved, the centralized management for national cybersecurity will be

able to ascertain the relevant authorities and hold them accountable for their responsibilities towards the efficacy and implementation of the various pillars of the strategy. However, the specialized efforts to signify responsibilities to the targeted groups might be more effective than a centralized management approach. Hence, further research needs to take place to ensure that cybersecurity purposes and the efficacy of the currently stated pillars are adhered to. In fact, further evaluation of the current risk management and incident responsiveness of the currently deployed cybersecurity workforce amongst organizations would have aided in the identification of gaps in education and skills development of the workforce.

2.11 Cybersecurity Workforce Skills and Demand

Due to the surging severity and alarming impact of cyber threats and attacks, the need and consequent demand for a competent and proficient cybersecurity workforce are inevitable. The UAE cyber threat landscape demands a responsive view from its cybersecurity professionals, thereby requiring them to acquire a certain set of skills and tools to equip them with the ability to respond to sophisticated cyber threats and attacks. Therefore, this section will explore literature and studies concerning the required set of skills for cybersecurity professionals and the pertaining significance of staffing cybersecurity positions. Simultaneously, with the rise in cyber threats and attacks, the literature review shall cover the increase in demand for cybersecurity skills and training needs regarding the growing complexity and traceability of cybercrimes.

The scarcity in qualitatively assessing the cognitive aptitude and competency of the cybersecurity workforce is summarized as a crucial dilemma for cybersecurity researchers. However, the combination of technical skills and social intelligence is implied

as effective to cater to the currently advancing cybersecurity landscape (Van Slyke C. , Clary, Ellis, & Maasberg, 2019). According to Dawson and Thomson (2018), the domain of the cybersecurity field itself is within the multi-disciplinary range of computer science, mathematics, economics, business, law, psychology and engineering. The knowledge for cybersecurity professionals requires not only networking through online devices but also catering to how different individuals interact with the devices (Loader and Thomas, 2013). The difference in how individuals interact with the devices tends to add to the complexity of the cyberinfrastructure (Von Solms and Van Nierkerk, 2013). Hence, this section shall emphasize the need to incorporate a range of technical skills and social intelligence to identify the approach in which they can harden the entity's cyberinfrastructure.

According to Dawson and Thompson (2018), the security provision roles as part of a generalized cybersecurity workforce framework includes network architects, software developers and computer programmers. Apart from the technical roles, the maintenance, operations, and governance of cybersecurity requires system administrators, knowledge management, security analysts, cyber analysts and network defenders (Dawson and Thompson, 2018). Moreover, given the research by Celeda et al. (2020), cybersecurity professionals must have proficiency in data security, software security and component security. The (Andre, 2016) research work elaborates on data security as gaining prolific competency in cryptography, forensics, data integrity and authentication while software security focuses on secure programming, testing and inspection along with in-depth knowledge of software development. In addition, the skills of component security require the professional to be adamant with the security of all different components integrated into the network system, specifically the design and reverse engineering of the system

(Celeda et al., 2020). Dawson and Thompson (2018) research affirm that cybersecurity professionals must have a high level of expertise along with self-professed expertise to be consistent with informal education supplementation. The (Blair, 2017) research requires the professionals to have sufficient mental flexibility and pattern-matching abilities along with analytical thinking skills to be proficient with network scanning, network mapping and vulnerability analysis. More specifically, network analysts amongst cybersecurity professionals must be good with intrusion detection which is complex by virtue. Lastly, the (Raajivan and Cooke, 2018) research requires the individuals to be team players as a group with diverse work roles and backgrounds so that they are better able to solve complex tasks.

2.12 Cybersecurity Skills Shortage

Recently, there has been rising publicity on the necessity of cybersecurity, especially in the need to train skilled cybersecurity practitioners (ESG - ISSA, 2020). Each year, top stakeholders in cybersecurity, such as principal business owners, managers, IT administrators, developers, and technology enthusiasts, host seminars and webinars while orientating the public on the benefits of digital security (ISSA, Cyber Securities Guidance Paper, 2020). The reason is that more than ever before, existing and upcoming technologies would demand robust security and error-proof cybersecurity protection (ESG-ISSA, 2021). However, despite the efforts made so far in creating consciousness of cybersecurity globally, wide margins still exist between the heights scaled so far and the gaps yet to be covered. According to the Enterprise Research Group, ESG (Oltsik, 2018), more than 70% of managers complained about the drastic shortage of cybersecurity professionals in their organization resulting in low productivity

and innovation. The (ISC, 2020) study shows a staggering shortage of 3.1 million cybersecurity professionals around the world. The gap is most significant in Asia with a shortage of 2 million individuals, followed by a shortage of 527,000 professionals in Latin America, 376,000 professionals in North America and 168,000 in Europe (ISC, 2020). Aside from the damaging decline in productivity, the lack of cybersecurity professionals exposed companies to cyber-attacks and severe threats (Kam, Menard, & Katerattanakul, 2018). Increased cyber threats also accelerated the creation of more disastrous spyware targeted at large business conglomerates and agencies (Cobb, 2018). Thus, in a bid to prevent most attacks, businesses end up spending huge sums and spending much more in recovery. Furthermore, the difficulty of detecting threats beforehand and confronting attacks further stresses the necessity of encouraging more attention to cybersecurity (Crumpler & Lewis, 2019).

In further analysis of their research, the ESG team, researching the cybersecurity skills shortage, specifically emphasized the worsening decline in four years leading to 2018 (ESG ISSA, 2018). In the first year, beginning with 2014, most research indicated a lack of cybersecurity personnel by 23%, which later rose consecutively to 51% by 2018. It is evident that there is a rapid shortage of cybersecurity skills, with each new year's decline superseding the previous year's (Furnel, Fischer, & Finch, 2017). For instance, out of most respondents interviewed in 2015 by ESG, 25% of them complained of threatening shortages of cybersecurity professionals, while 46% of respondents also complained about the same need in 2016, in 12 months (Herjavec, 2021). In the latest survey conducted in 2021 by ESG, over 57% of the organizations reported a shortage of cybersecurity professionals (ESG ISSA, 2021). Hence, these reports indicate a

deteriorating situation that will worsen in a couple of years if the problem is not addressed. Therefore, especially in the changing cyber landscape, it is essential to regenerate talents and skills in cybersecurity that will consistently bridge existing gaps and provide sustainable solutions to skills shortages (Funnel & Bishop, 2020).

Moreover, the threats posed by decreasing number of talents in cybersecurity protection are much more pronounced and alarming in developed nations owing to the massive data generated, processed, stored, and shared in such countries as the USA, China, Russia, Germany, UK, and other significantly developed economies. Additionally, the interconnectedness of their technologies presents more substantial risks and worries as to the safety of the servers and web hosts that house data (Angafor, Yevseyeva, & He, 2020). The fact that more challenging cyber issues face first-world countries does not imply the absence of threats in developing and third-world nations, but the former faces more significant risks due to numerous factors (Smith, 2016). One crucial risk factor faced by advanced economies is intelligent technologies and intelligent devices that collect data regularly (Center for Strategic and International Studies, 2016). These technologies will always demand tighter security to offer them protection since cyberspace constantly evolves (Caulkins, Marlowe, & Reardon, 2018).

As a defensive measure, many technical firms, business leaders, including CEOs, are now taking proactive measures to withstand the current and predicted lack of cybersecurity expertise (Carlton, 2016). However, despite the number of pragmatic steps taken, the ensuing lack of cybersecurity professionals is apparent and is becoming more pronounced in recent years. This shortage has attentively created alarms that technology experts are already responding to by building automated technologies that detect and

instantly terminate threats and ensure that future occurrences are prevented (Caulkins, Marlowe, & Reardon, 2018). However, most of the efforts aren't concerted but rather individualistic and more regionalized than globalized due to global socio-economic imbalances. First, the technological gaps existing between emerging economies and economic powers threaten the collaboration needed to collectively build skills in cybersecurity (Blair, 2017). Furthermore, over the past couple of years, political and socio-economic inequality have further exacerbated and widened the existing gaps, thereby creating disequilibrium. Secondly, most underdeveloped nations may decelerate training more cybersecurity professionals (De Zan, 2020). Usually, technology leaders in underdeveloped countries lack the human and material resources and technical know-how necessary to build strong cybersecurity controls, and they depend on foreign experts (Shires, Enacting expertise: Ritual and risk in cybersecurity, 2018). For instance, the importation of the services of insufficient cybersecurity experts from the US to South Africa will create a troubling deficiency in the US while not satisfying the rising demands in South Africa. Hence, every country, region, and sector need to train and equip more cybersecurity professionals who can withstand constantly emerging cyber threats in cyberspace (McCubbrey, 2020).

Furthermore, improved development of cybersecurity practitioners and technologies for cyberspace protection would not be efficient for protecting the vulnerable digital world. Therefore, the Information Systems Security Research Association (ISSA, 2020) suggests consolidating integrated web securities and analytics as a panacea to predicting and confronting cyber-attacks. Moreover, irrespective of the size, industry, location, and organization, the shortage of cybersecurity talents impact everyone.

Therefore, in addition to the cybersecurity staff shortage, insufficient technologies can holistically manage sudden incidents by appropriately utilizing advanced technologies. It is, therefore, with this context that data science (DS), machine learning (ML), and artificial intelligence (AI) play crucial roles in automatically handling cyber-attacks and threat incidents across the web and remote servers (ECSA, 2017). However, the insufficiency of AI tools can be pardoned, but there is an urgent need to develop more advanced tools that can handle unusual cyber-attack incidents using the insights derived from the data. Thus, a more data-driven approach to building formidable cyberspace firewalls and training professionals must be adopted (Reffold, 2020).

Furthermore, the drastic shift of attention from human-controlled cybersecurity to machine-regulated cyber protection has become predominant even in the next few years. Therefore, the future of cybersecurity must extensively incorporate the help of analytics and automation to manage cyber threats accordingly. Recent research also indicates the cruciality of cloud computing as an approach to cutting costs, saving time, delegating controls, and simplifying security infrastructures (Van Slyke, Clary, Ellis, & Maasberg, 2019). From the human perspective, there is also a reasonable assumption that better work compensations, career development, training, and mentoring can significantly improve the building of more and improved cybersecurity practitioners.

Despite the high hopes and seemingly practicable future projections on the brighter side of cybersecurity, research evidence clearly shows some irreparable gaps in the nearest future. In 2017, (Cyberbit, 2018) reported that the cybersecurity market would be worth 202.36 billion USD by 2021, with about 200,000 unfilled cybersecurity jobs in the United States, while Forbes also projected 1.5 million unfilled positions by 2019 (Sayegh,

2020). These statistics depict the huge gaps yet to be filled while presenting more lucrative horizons to be explored. And with series of emerging internet threats and digital attacks, the shortage in cybersecurity skills creates a state of emergency. Even significant players of the industries continue to express the difficulties in recruiting, training, and remunerating talented cybersecurity experts knowledgeable enough to deliver excellent security services (Sutherland, 2018).

Moreover, beyond hiring new cybersecurity professionals, it is also tasking to train and mentor new cybersecurity talents custom to the often-complex cybersecurity needs of an organization. In essence, reskilling professionals to meet and even exceed the demands of an organization may not be relatively cost-effective, especially when experts are not offering excellent services. In today's information and communication technology (ICT), we see other computer professions preceding cybersecurity in order of popularity (Chouliaras, Kittes, Kantzavelou, & Maglaras, 2021). Thus, based on a (Cyberbit, 2018) report, skills concentrations in IT are found around Lead and Software engineering, information security, and consultancy topping the list while cybersecurity constantly remains at the bottom. Also, on a job shortage chart, the insufficiency of cybersecurity workers maintained a consistent rise by 9% above mobile application development, business intelligence, and enterprise mobility management. Speaking on the alarming shortage of skills in cybersecurity, Frost and Sullivan lamented the roles of humans in ensuring that even some automated analytics tools perform tasks effectively (Chavis & Syed, 2020). Thus, according to their detailed research, advanced and self-regulated technologies can't effectively work without human controls. Hence, there is a need to train more cybersecurity experts acquainted with the volatile cyberspace. Technologies will

execute tasks under the tutelage of professionals writing the programs and giving the commands.

Moreover, since we live in an age where governments, organizations and businesses face complex cybersecurity threats, employees with the needed cybersecurity skills must combat cybercriminals and win the battles against cyber-attacks (Maennel, 2020). Therefore, first, it is critical for businesses and leaders of industries to analyze and determine the degree of cybersecurity skills shortage before investing in the development of new talents. However, tech-savvy young people can maximize internet and computer resources to bridge the widening gap if only the optimum skills development pathways and training are accessible (Maleh, Shojafar, Alazab, & Y, 2021). Therefore, the concerns for protecting confidential, classified, and critical data and resources from unauthorized access should drive concerned stakeholders to increase investments in intensive and extensive training of future cybersecurity professionals that emphasizes practical application of the learned principles.

2.13 Current Solutions for Cybersecurity Skills Gap

With the apparent rise in cyber threats and attacks, the need to bridge the cyber security skills gap has become a critical concern in order to meet the sheer demand of businesses, governments and private institutions. Researchers recognize the lack of investment, innovative home-grown cybersecurity initiatives & campaigns, and weak public policy efforts to narrow down the widening gap. From mass phishing campaigns to targeted nationwide attacks, the severity of the cyber-crimes and the increasing traceability of the cybercriminals require the supply of qualified and competent cybersecurity professionals. Hence, this section will elaborate on the current state of the

cybersecurity skills shortage and the solutions to bridge the gap readily and in the long run.

(Cobb, 2018) Addresses the increasingly immediate concern for the significant cybersecurity skills gap and the hammering obstacles in mediating the gap effectively. The study defines cybersecurity skills gap as the problematic shortage of meeting the requirement for cybersecurity expertise. The study uses empirical evidence from reports such as Cisco and Human Capital Crisis Report to signify the depth of the problem (Caldwell, 2016). Furnell et al. (2017) elaborates that in addition to the shortage of highly technical skilled workers, there is a pressing need for individuals who can operate and support different network systems in order to create a sophisticated set of tools that can prevent, detect, mitigate and reconstitute the damage and impact of cybercrimes. The study by Crumpler and Lewis (2019) criticizes the reliance on the private sector for cybersecurity development as governments do not focus their strategies and investment on developing the nation's cybersecurity workforce. Further, the study emphasizes on the lack of educational and training programs concerning cybersecurity to harness efforts in developing the required expertise (Cobb, 2018).

Moreover, according to CSIS (2019), the evaluation of the US cybersecurity workforce revealed the shortage of education and training programs to assist the need of high-skilled technical roles as they represent most of the gap. More specifically, CSIS surveys revealed that only half of the graduates in cybersecurity degrees were qualified for the workforce positions due to the irrelevance of the cybersecurity related educational programs across the United States (Francis et al., 2016). The graduates are perceived to lack practical experience and a primary understanding of cybersecurity methodologies

(CSIS, 2019). Therefore, CSIS details the need for on-the-job training for cybersecurity graduates along with challenging competency in skills such as team working, problem solving and social interaction. Furthermore, responses from NIST heightens on the need for fundamental set of skills to build up the specific knowledge for the required roles (NICE, 2021). Hence, researchers recognize the need for cybersecurity programs to be focused on cybersecurity policy planning, compliance audits and cybersecurity laws to mediate the financial and social impact of the attacks on an organization's threat landscape (Zan, 2020). Furthermore, studies identify a shortage in professionals' skills and the range of expected knowledge, skills, and expertise for the required job (Rotim and Komnenic, 2020). Hence, the pressing need to build a multi-disciplinary cybersecurity workforce requires both short and long-term solutions (Vogel, 2016).

2.14 Current Research Efforts to Bridge the Cybersecurity Skills Gap

Addressing the pace of relevant technological advances and the evolving nature of cyber threat landscape, remedial solutions should be introduced towards incorporating a multi-disciplinary approach to create interest regarding developing technical skills amongst students as well as current cybersecurity practitioners. Researchers have elaborated on the following solutions:

2.14.1 Gamification

(Scholefield and Shepherd, 2019) elaborates on gamification techniques to educate users regarding cybersecurity awareness via the use of password applications. Due to the increasing user reliance on authentication mechanisms such as biometric authentication, fingerprint-based systems etc., the study illustrates that gamification techniques can help build up end-user security awareness. For instance, SAPS (Status,

Access, Power and Stuff) utilized gamification in the delivery of rewards. The mechanism integrates a leader board to allow users to compete, in addition to loyalty schemes for keeping the users engaged. The study involves the use of gamification techniques in university-level courses and through a combination of rewards to improve knowledge acquisition. Furthermore, another cyber security-based games such as Webonauts Internet Academy can be used to make awareness about online etiquette and promote continual engagement and development of cybersecurity skills. Research studies highlight summer camps such as GenCyber that has launched through National Security Agency of US to raise student's interest in regards to computing and social engineering. Furthermore, applications such as NoPhish can be used to aid users in identifying phishing links and create informed decisions of good security practice for cyber threats (Scholefield and Shepherd, 2019).

Moreover, Fink et al. (2013) elaborate on gamification for measuring cybersecurity situational awareness. The study uses empirical evidence of The Pacific Rim Collegiate Cyber Defense Competition for observational experiments. The competition utilized team performance in an independent manner through digital and audio recorders to assess the situational awareness of students and resulted in improved team's cognition and configuration skills (Fink et al., 2013). Furthermore, Yonemura et al. (2017) utilized the practice of information, communication, and technology (ICT) security through an emphasis on operational technology (OT) skills. The study used comprehensive security training followed by gaming security teaching materials to effectively measure the skills level of the participants (Yonemura et al., 2017). According to the authors of Wolfenden (2019), the technique proved useful in learning the basics of cybersecurity concerning

critical infrastructure in a short period, hence, illustrating the efficacy of gamification techniques. For instance, KIPS, a game based on gamification theory, levelled learning scope for students from varied educational backgrounds through teaching the fundamentals rather than building deep expertise regarding cyber security (Wolfenden, 2019). The experiment conducted by the researcher in this research study utilizes the gamification platform in order to validate the upskilling of the technical hands-on skills amongst students.

2.14.2 Apprenticeship

Thompson et al. (2019) specified that the usual cyber career path requires three to four years for completion of graduate degree followed by various training programs for specialization. Hence, the study suggests apprenticeship as a more effective hands-on approach in order to give practical experience to the cybersecurity professionals. Similar to traditional apprenticeship programs, the program shall focus on developing the fundamentals and then working towards the more complex tasks. According to the study, apprenticeship offers the use of skills and experience to further their experience with an increase in high-value activity. The theoretical side of cybersecurity is further addressed through practical experience during such programs. Hence, a blended approach can be developed through hands-on experience with academic teaching and testing in order to heighten developing qualified and proficient cybersecurity professionals. Further, the inclusion of essential cybersecurity skills and developing the extent of their existing personnel help in training for the provision of resilient cyber protections. The research author further elaborates those apprenticeships can enable organizations to acquire new candidates and train them simultaneously. Directing the organization's investment will

help to effectively regulate their aptitude on a regular basis and thus, evaluate the best ones for promotion (Boopathi et al., 2015). However, researchers necessitate the employers to work as consultants to the employees in order to develop the skills that is best suited to the capacity of the candidate. Hence, the program provides a practical platform to evaluate cybersecurity professionals and maintain proficiency and competency amongst the current cybersecurity workforce of the organization (Thompson, 2019).

Furthermore, (Vasileiou, 2021) explores aid in teaching a collaborative work environment for cybersecurity professionals with increased focus on their education and skills employability. In the case of UK, the graduates will not rely on the fundamental skillset and the apprenticeship but will focus on fulfilling job requirements and gaining additional expertise regarding the technological advances in cybersecurity (Beyer and Brummel, 2015). According to the study, the degree apprenticeship model was coherent in communicating the link between theoretical learning and the practical implementation of the learning, thus, leading to improved employee attainment and retention (Vasileiou, 2021).

2.14.3 Capture the Flag Platform

Due to the increased cybersecurity workforce demand, Ford et al. (2017) summed the Capture the Flag (CTF) platform as one of the thriving platforms in supporting the education and awareness of cybersecurity skills in an interactive manner. According to the study, the CTF unplugged project planned to raise awareness in a realistic fashion by teaching students who had no or minimal knowledge concerning cybersecurity (Coventry et al., 2014). The program acted as an awareness campaign for highlighting different

cyber-security challenges by focusing on problem-solving skills. The platform was reported to provide a deeper understanding of the significance and influence of cybersecurity and raise its awareness amongst the youth. The program focused on fundamental security concepts, problems and solutions through a holistic series of interactive lessons and hands-on training. The program offered a practical experience along with theoretical learning, incorporating enhanced student interest and a realistic approach to common cyber-attacks (Hulatt and Stavrou, 2021).

Furthermore, literature shows that the CTF platform provided the resources required and focused on developing the competency of the participants involved with equal access to the required equipment and tools (Colon Perez, 2018). Hence, CTF provided an approach to capture maximum learning within the process through the inclusion of both technical and logical activities while supporting the development of their critical thinking skills (Craigien, 2014). More specifically, (Ford et al., 2017) specified the inclusion of activities such as cryptography, reconnaissance, forensics, reverse engineering, and steganography. Therefore, the activities aided in providing a comprehensive experience of using different techniques without the need for prior knowledge or expertise (Raman et al., 2014).

2.14.4 Simulation

Additionally, (Jalali et al., 2019) signified the use of simulation game experiments for the development of cybersecurity capabilities. The research indicated the significance of proactivity in cybersecurity capability development in order to stress a reactionary approach and reduce the failure rates of resisting cyber threats and attacks. The research

has shown that simulations facilitate the analysis of learning effects within complex organizational environments (John et al., 2020). The simulation experiment of (Jalali et al., 2019) focused on strategic management and organizational science in order to optimally utilize the heterogeneity in the performance of the participants. Therefore, in order to develop an adverse attitude towards dealing with the uncertainty of cyber incidents, the research indicated that the simulation model dynamically incorporates the eco-system of computerized systems while covering all its vulnerabilities (Svabensky et al., 2018). The study summarized that the investments in the preventive capabilities alone for the cybersecurity professionals would impact the increased competency of their interaction with cyber incidents along with becoming proficient in the complexity of the decision-making process regarding risk protection of the organization (Corradini, 2020). Furthermore, the research reported findings that the simulation is effective in analyzing the patterns in cyber incidents and allocating resources pertaining to optimal efficiency for the organization (Jalali et al., 2019).

2.15 Current Research Gaps in filling the Cybersecurity Skills Gap and its Remedial Approaches

Although research studies and literature regarding the current state of cybersecurity skills gap and the approaches to narrowing down the gap are coherent in the short and long term, the effectiveness of the approaches relies upon various mystifying factors. The approaches need to accommodate the fact that the time frame for bridging the gap will be extended due to the severity and complexity of the cyber threat landscape. Hence, initiatives such as gamification or simulation approaches need to be incorporated along with educational programs for the solution to be holistic and effective.

Moreover, the research focuses on the optimal efficacy of the programs without identifying the assumptions behind it such as *ceteris paribus* for other progressive careers, investments behind the installation and monitoring of the approaches, the role of the government entities in strategizing the reduction in the skills gap and efforts required to retain the interest of cybersecurity professionals in the consistent improvement of their skills. Furthermore, policies regarding the integration of public and private sectors in accumulating their expertise and capital in developing perfectly interesting and applicable education and training programs should be part of the research approaches. Hence, research gap exists in assuming the currently untapped cybersecurity aptitude and potential without evaluating the willingness of the individuals to be part of the cybersecurity workforce.

2.16 Theoretical and Conceptual Framework

Building further on the existing research efforts, the theoretical framework explored by this research work relates to using a gamification platform to enhance the hands-on technical skills amongst undergraduate students who majored in cybersecurity. This research attempts to fill a void in the literature by exploring the effectiveness of using a technical gamification simulation platform to enhance hands-on technical skills amongst cybersecurity undergraduate students. The research study employs the qualitative grounded theory design to understand and measure the improvement in the hands-on technical skills by examining the experience a number of participants had while undergoing the experiment of having access to the gamification platform. The sample size for this research was mindfully selected from a pool of 3rd and 4th year undergraduate

students majoring in cybersecurity from various renowned universities across the United Arab Emirates.

The experiment was applied to the selected participants and consisted of three phases: assess, train, and perform. The data (i.e., the experience of the participants) was collected from all three phases. The first phase, the assess phase, was in form of responses to face-to-face interview questions. The second phase, which was the training phase, was about results collected from the dashboard scores. This is after the participants have had access to the technical simulation gamification platform. Finally, the performance phase involved results that were in the form of survey questionnaire responses.

The conceptual framework that was applied for this research study was to identify the cause-and-effect relationship of our stated research questions of using technical gamification simulation platform in improving senior year students' hands-on technical cybersecurity skills is based on assessing their skills pre and post conducting the training experiment. The research study focused on understanding, measuring, and evaluating the way the participants used the gamification platform to complete the assigned technical challenges. In addition, the study measured the use of gamification platform that improved the confidence level of the participants in their technical skills. In addition, the study measured the shared experiences of the participants as regards introducing such a gamification platform ahead of time within their academic undergraduate program to gain superior technical skills while completing their academic coursework. Furthermore, the study measured the participants' eagerness to continue using the technical gamification

simulation platform after completion of their academic journey to continue building their technical hands-on cybersecurity skills and building new ones over time.

After going through the historical literature, limited research studies conducted showed the effective use of a gamification simulation platform to instruct hands-on technical skills to students in an academic environment. This has highlighted the lack of information needed to integrate such kind of improvement into academic environments. Hence, this research study took high interest in working on this approach to make purposeful research conclusions and filling the void in the literature. In addition, the researcher aimed to introduce new ways that can be added to the current academic undergraduate programs that can provide improvement in the quality of fresh graduates that are completing the cybersecurity undergraduate programs in the universities in the UAE and are market ready as skilled cybersecurity professionals.

The Kolb's experiential learning theory (ELT) (Kolb, 2015) is the basis of the theoretical framework for conducting this research study. Kolb's theory focuses on the thought that the best way to learn anything is by creating opportunities and real-world environments where students have the ability to experience and learn by doing (Kolb, 2015). The aim of this research study is to stress the essence of the introduction of the use of a technical gamification simulation platform that is available around the clock whenever and wherever the student is situated during their academic studies. Also, this research aims to show that a technical gamification simulation platform shall enhance the technical skills of the students, which shall eventually narrow down the skills gap and introduce early adoption of computing fresh graduate students into the technical career market.

2.17 Chapter Summary

This chapter sums up the overview of cybersecurity and its implications on the outlook of an economy due to the surging occurrence of cybercrimes, ranging from phishing campaigns to nation state cyber-attacks. The review also provides insights into the key concepts of cybersecurity to offer a deep understanding of the cyber threat landscape globally and specifically in the case of the UAE. Also, the chapter shows that the in-depth view of the nature, severity, complexity and impact of the cyber-attacks in the UAE in contradiction to its existing cybersecurity talent shortage and the need for adequate execution of its cohesive national cybersecurity strategy is pivotal to understanding the future outlook of UAE cyber threat landscape. The literature review was relevant and coherent with the objective of detailing the significant information as well as stressing the research gaps to enable further studies.

The outlook of the UAE cyber threat landscape presents a summary of the need for growth and development in the educational and training aspects regarding cybersecurity and the increasing need for understanding the increasing surge in the rate of cyber-attacks. The sections offered a chronologically coherent and detailed view of cybersecurity and offered transparency in understanding the complexity of different types of cyber threats. Moreover, the chapter reviewed examples and evidence of different cyber incidents that impacted various sectors significantly, thereby, helping to identify the future challenges to the field of cybersecurity. Furthermore, the chapter summarized the key concerns regarding cybersecurity and aided the understanding behind each solution required amongst the cybersecurity professionals along with the remedial approach to incorporate the relevant skills in the workforce. The evidence from the UAE cybersecurity

workforce framework is effective in understanding the future scope for the skills identified and the intended consequences if the skills gap extends further. In addition, the chapter provides support for justifying the strategic objectives, vision, aspirations, pillars and tools specified in the UAE National Cyber Security Strategy and Incident Response Plan along with identifying the factors that have been overlooked.

The chapter cohesively summarized a deep understanding of the field of cybersecurity and the need for cybersecurity workforce training and development initiatives amongst different industry sectors. The need for a cybersecurity workforce in mitigating the rise of cyber threats and attacks along with elaborating on the cyber threat landscape are emphasized to a great extent in the chapter. The chapter also described the further assessment of the identified research gaps along with forecasting the future prospects in the field that may differ within organizations and educational systems. The chapter also presented an analysis of the relevant literature available on cybersecurity in addition to addressing the general trend towards sophistication and complexity of cyber-attacks. The chapter concluded with presenting the conceptual framework used in this research work.

Chapter 3: RESEARCH METHODOLOGY

The purpose of this qualitative grounded theory research is to understand and explore how the use of the technical gamification simulation platform can be used to enhance the hands-on technical skills of undergraduate students majoring in cybersecurity. The results from this research work shall lead to introducing new ways of assisting the undergraduate cybersecurity academic program in producing skilled cybersecurity professionals. A sample of 9 students who are in their 3rd and 4th-year and actively enrolled in the cybersecurity undergraduate program were mindfully selected using purposeful sampling from a total population of 50 students from various renowned universities across the United Arab Emirates (UAE). The selection of students for the experiment was determined by rigorously interviewing them, both academically and technically.

In this chapter the research approach and design are explained. The upcoming sections elaborate on the research methodology employed and the reasons for the selected research design. Also, it outlines the research approaches, scope of the study, the background of the technical gamification simulation platform, target population, and sample size and procedures. Finally, this chapter encompasses both data collection and data analysis and elaborates on the procedures used to satisfy the objectives of this research work, a qualitative research design was employed.

3.1 Research Design

This study leverages the grounded theory methodology data analysis techniques to identify patterns or themes (Creswell & Guetterman, 2019) that will determine how

integrating a gamification platform alongside a traditional cybersecurity educational program will enhance the hands-on technical skills of undergraduate students. In the context of information systems (John W. Creswell, J. David Creswell, 2018) noted that there are three distinct research methods, i.e., the qualitative research method, the quantitative research method, and the combined/mixed research method.

The gathering and investigation of statistical data is part of quantitative research. Quantitative research allows data to be quantified or statistically explored and explained (Thomas Edgar and David Manz, 2017). Quantitative data is routinely used and examined by a descriptive researcher (Oates, 2006), and it is provided by critique and hermeneutic scientists. Researchers who follow this research method use an instrument to measure the variables in the study. Examples of quantitative data collection instruments are survey questionnaires, standardized tests, and checklists that are used to observe and measure an individual's behavior (Creswell & Guetterman, 2019).

In quantitative research (Creswell & Guetterman, 2019) stated that researchers study independent variables to see what effect they have on the outcome. For example, for the purpose of this study in order to evaluate or validate the outcome of prior knowledge as opposed to the gaining or advancement of advanced knowledge the researcher can use the control and treatment groups. (Creswell & Guetterman, 2019) defines the treatment variable as another form of independent variable that can be used in educational experiments. For example, the researcher treats one group of participants to a specific experiment and treats another group with a different set of activities. This is to verify whether the group that went through the treatment experiment scores in any way differently than on the dependent variable than the group that did not receive the

treatment experiment. This is one of the quantitative research methods that the researcher could have used to strengthen the outcome of the experiment.

On the other hand, (Creswell & Guetterman, 2019) stated that qualitative research is best suited to address a research problem in which you do not know the variables and need to explore. The collection and evaluation of descriptive data is part of qualitative research and in such a research method, data is collected to learn from the participants in the study. The researcher develops forms that pose general questions so that the participants in the study can provide answers. An open-ended stance interview, personal observation, and a survey questionnaire are used to gather qualitative data. A participant's experiences, views, sentiments, and expertise are directly quoted during the interviews. Observed data includes extensive assessment of participant's activities, behaviors, actions, and experiences (Michael Quinn P, 2014). (Creswell & Guetterman, 2019) Further explain the qualitative research as when an investigator seeks to gather information on a single concept known as the central phenomenon. Furthermore, in qualitative research an investigator asks participants in a study to share ideas and build general themes based on those ideas. In addition, the investigator aims to seek a deeper understanding of the views of one group or single individuals (Creswell & Guetterman, 2019).

Mixed methods research, is a research design that includes research philosophy along with inquiry techniques. As a methodology, it entails a research philosophy that influences collecting data and assessment and the combination of qualitative and quantitative methods in a single study or set of studies. Its core idea is that combining quantitative and qualitative methods yield a greater grasp of research challenges than

either method alone (John W. Creswell, Plano Clark, 2018). Mixed method research outcome can also be employed for this experiment in order to strengthen the outcome of the experiments results.

Thus, the research problem this study tackles is how the introduction of the technical gamification simulation platform (TGSP) alongside the traditional undergraduate cybersecurity academic program requires both an exploration (because we need to explore how the introduction of the TGSP platform will raise the hands-on technical skills set amongst the undergraduate students) and an understanding (because of its complexity) of the process to truly introduce such a platform alongside the curriculum. As the aim of this research work is to learn more from the participants in the study through exploration, hence, a qualitative research method was employed in this research work. A central phenomenon as defined by (Creswell & Guetterman, 2019) is the concept or the process explored in qualitative research. In this research, the central phenomenon being understood and explored is that of enhancement of hands-on technical skills of the students. In addition, qualitative research is an emerging process. (Creswell & Guetterman, 2019) Defined an emerging process as a situation where the intent of purpose of a study may change during the process of inquiry based on the responses of the participants of the study. This is because the researcher learns the participants' views rather than impose his or her views on the research situation.

As defined by (Creswell & Guetterman, 2019), research objectives are statements of intent used in quantitative research that specify the goals that the investigator plans to achieve in the study. Because this research work is a qualitative

study, there are no research objectives stated, but the focus is given to research purpose and research questions.

Research questions, as defined by (Creswell & Guetterman, 2019), are questions in both quantitative and qualitative research that narrow down the purpose statement to specific questions that researchers seek to answer. In qualitative research, the questions examine the central concept/phenomenon (Creswell & Guetterman, 2019). On the other hand, hypotheses are statements in quantitative research in which the investigator predicts an outcome of a relationship among attributes (Creswell & Guetterman, 2019). Considering that this study is employing the qualitative research method, only the research purpose statement and research questions will be discussed without the need to list down the hypotheses. As (Creswell & Guetterman, 2019) stated in quantitative research, hypotheses are used. In qualitative research, hypotheses are not used; instead, researchers use only research questions. This is because researchers use hypotheses using statistics and statistics are not used in qualitative research.

Researchers use both purpose statements and research questions to alert the readers to the main direction of the study. A purpose statement in qualitative research indicates the intent to understand and explore the central phenomenon with specific individuals at a certain research site (Creswell & Guetterman, 2019). Hence, the purpose of this qualitative grounded theory research is to understand and explore how the use of the technical gamification simulation platform will enhance the hands-on technical skills of undergraduate students that are majored in cybersecurity academic

programs. This study uses the grounded theory methodology with a series of open and in-depth one-on-one interviews, survey questionnaires, dashboard participants scores, and observation to guide the collection of extensive and rich data to attain the goal of the research.

(Creswell & Guetterman, 2019) Defined qualitative research questions as open-ended, and general questions that the investigator would like it to be answered during the course of the study. Qualitative research is composed of two types of research questions. A central question and sub questions. (Creswell & Guetterman, 2019) Defined the central question as the overarching question the investigator aims to explore in a research study. While sub questions, on the other hand, tend to refine the central question into sub questions to be addressed in the research work. These sub questions provide greater specificity to the questions in the study. Sub questions can either be “issue sub questions” or “procedural sub questions”. In this qualitative study, procedural sub questions form is used by the researcher. In this form of sub questions, the researcher knows what steps of analysis will be (Creswell & Guetterman, 2019). A procedural sub question formed study provides the readers of the study with a more precise understanding of the steps taken for analysis.

Hence, the research central question this qualitative study intends to provide a factual answer to is:

Can the use of the technical gamification simulation platform (TGSP) upscale the hands-on technical skills amongst cybersecurity undergraduate students?

The following are research sub questions to understand and explore during this study:

- **RQ1:** *What are the students' hands-on technical skills experiences once they complete their 4th-year cybersecurity undergraduate degree program?*
- **RQ2:** *What are the students' hands-on technical skills experiences once they complete the cyber range gamification platform scenarios (i.e., both Battle Rooms and Missions)?*
- **RQ3:** *What are the students' hands-on technical skills experiences once they complete the capture the flag gamification platform scenarios?*
- **RQ4:** *What are the student's experiences on the effective training platform considering the cyber range and/or capture the flag?*
- **RQ5:** *How can the hands-on technical skills acquired by the students using the technical gamification simulation platform can be validated using the dashboard?*

3.2 Grounded Theory Design

Grounded theory design is defined as examining a number of individuals, all of whom have experienced an action, interaction, or process (Creswell & Guetterman, 2019). This research design is best suited for this research work, as our experiment is devised to be applied to the participants of the study to experience the central phenomenon that is to explore the enhancement in the hands-on technical skills of the undergraduate students over the course of an 8-weeks experiment program. Furthermore, (Creswell & Guetterman, 2019) point out that grounded theory design is a systematic, and qualitative procedure that researchers use to generate a general explanation (grounded in the views of the participants, called a *grounded theory*) that explains a process, an action, or an interaction among people. The researcher followed

the systematic steps of collecting the data, developing and relating the categories / themes of information, and composing a figure or a visual model that portrays the general explanation (Creswell & Guetterman, 2019). This composure of the visual model is in the form of designing and developing the cybersecurity skills performance dashboard that provides a true assessment of the hands-on technical skills acquired by the participants in the study during the experiment program. In addition, the research also constructed predictive statements about the true experiences shared by the participants in the study. Thus, the grounded theory research design is considered an ideal method of identifying and capturing the enhancement of the hands-on technical skills of the undergraduate students whilst using the technical gamification platform.

The grounded theory methodology initiates with inductive data and involves iterative steps of data analysis. Further, it utilizes comparative analysis to facilitate the interaction between the data and the researcher (Charmaz & Henwood, 2017). This shared data between the data collected and the researcher supports identifying underlying themes and phenomena within the qualitative data collected to support the study (Charmaz & Henwood, 2017). Research findings are supported by inductive reasoning as a core characteristic of the grounded theory methodology (Creswell & Guetterman, 2019). The use of qualitative grounded theory methodology to collect and analyze data assisted in tackling the research problem. This is because the goal of the research is to gain insights, explore, and understand how to enhance the technical skills of undergraduate students and shorten the skills gap problem.

3.3 Population and Sample Size

In this section of the chapter the research study population and sample size shall be presented. In addition, this section will explain in detail the approach used for the participant selection for this research experiment.

3.3.1 Population and Target Population

As defined by (Creswell & Guetterman, 2019), a population is a group of individuals who possess one characteristic that distinguishes them from other groups. Researchers do not always study an entire population either because they cannot identify the individuals or because they cannot obtain lists of names. In practical operational terms, researchers study a *target population* or what is known as a *sampling frame* (Creswell & Guetterman, 2019). The target population is an actual list of sampling units from which a sample is selected. The sample is the group of participants in a study that a researcher selects from the target population and from which the researcher can generalize for the target population. Researchers ensure that the sample represents the population to certify that claims or inferences can be drawn from the sample to the population.

Hence, this qualitative study's target population was undergraduate 3rd and 4th-year students from across different universities across the United Arab Emirates who are actively enrolled in an undergraduate academic cybersecurity program. The selected participants needed to have a cumulative grade point average (GPA) of 3 or above and need to be a United Arab Emirates' National. The researcher ensured the drawing

inferences from the sample of the population by following the factors mentioned by (Salant & Dillman, 1994):

- *To reduce coverage errors, have a good sampling frame list* – the researcher selected participants that are all majored in cybersecurity. The sample includes both genders (i.e., male and female), participants from 4 different universities across the United Arab Emirates, participants with an excellent academic status in terms of GPA of 3.0 and above, have a good foundational technical knowledge, are 3rd and 4th-year students, and are all UAE nationals.
- *To reduce sampling error, select as large a sample from the population as possible* – the researcher used intensity sampling in order to select the sample size.
- *To reduce measurement error, use a good instrument* – the researcher used a good instrument that had clear, unambiguous questions and response options to encourage the participants in the study to respond and answer correctly and honestly.
- *To reduce nonresponse error, use rigorous administration procedures to achieve as large a return rate as possible* – the researcher ensured adequate administrative procedures were put in place to increase the response return rate.

3.3.2 Participant Selection

Intensity sampling is defined as the process of selecting or searching for rich or excellent examples of the phenomenon of interest. The researcher in this study selected

a small yet effective number of participants who exhibit depth information and knowledge of the cybersecurity field. As (Patton, 2015) points out, intensity sampling requires prior information and exploratory work to be able to identify intense examples.

This qualitative research study employed the purposeful sampling procedures of intensity sampling, with a sample size of 9 selected participants for the study. The sample included participants who:

1. Pursue their undergraduate degrees in cybersecurity;
2. Are 3rd and 4th-year students;
3. Study at different universities across the United Arab Emirates;
4. Are UAE Nationals;
5. Have an excellent academic status of GPA of 3.0 and above;
6. Have a good foundational technical knowledge & skills; and
7. Include both genders (i.e., males and females).

The selected universities for this experiment were, Khalifa University (KU), Higher Colleges of Technologies (HCT), Zayed University (ZU), and Abu Dhabi Polytechnic Institute (AD PolyTech).

One of the main reasons to select high-achieving students to this experiment was because the participant count was limited to 9 participants and the researcher wanted to ensure that the selection of participants was based on excellent academic status to ensure the interest of the participant to take upon the experiment seriously and to conduct each and every scenario / challenge as and when these are assigned.

The sample selection process was as follows.

1. The dean of the cybersecurity undergraduate academic program for every university mentioned above was contacted to request for their 3rd and 4th-year undergraduate students list who have an accumulative grade point average of 3.0 and above to contact the researcher if they want to be part of the experiment program.
2. The interested students willingly contacted the researcher and a date and time were scheduled to move to the next step of being interviewed and screened.
3. Once, the researcher identified the list of 50 undergraduate students, the date and time were scheduled for the intensive technical interview and screening to select the sample for the study.
4. The interview with every student lasted for 45 minutes. It started with an opening question to understand more about the student, their background, their technical achievements and technical projects they accomplished during their time in the university, and the technical challenges faced.
5. Further on, the interview had a second part to it which was testing the technical knowledge of the student and their ability to explain technical infrastructure. The purpose of conducting such a thorough technical interview was to be able to mindfully select or the research study participants who have the basic technical skills to be on boarded on the technical gamification simulation platform.
6. From a pool of 50 undergraduate students, only 9 were selected to be participants for this research work. Appendix 1 presents the template for the interview questions for participant selection for this research study.

7. The selected 9 participants as the sample size for this study consisted of both genders, male and female (i.e., 4 females, and 5 male participants).
8. In addition, all the participants were UAE nationals and had a grade point average of above 3.0.
9. Out of the 9 participants, seven (i.e., 3 females and 4 male participants) were 4th-year undergraduate students and two participants (i.e., 1 female, and 1 male) were 3rd-year undergraduate students. The reason 3rd-year undergraduate students were selected was to understand their experience whilst having access to the TGSP and the enhancement observed to their technical skills, to understand how early the introduction of TGSP can occur alongside the academic program.
10. The 9 participants were selected from four different universities to explore the different technical skills and knowledge that students brought to the experiment.
11. The distribution of participants as per the university they pursued their undergraduate program were as follows: (3 females from ZU (3rd and 4th-year), 1 female from KU (4th-year), 3 male participants from AD PolyTech (4th-year), 1 male from ZU (4th-year), and 1 male from HCT (3rd-year)).

(Creswell & Creswell, 2018) state that the selection of *n* participants for a specific research study shows that the selected participants reflect the broad group of the total population from which they have been chosen. Purposeful sampling strategies were utilized to select the distinguished sample for this research study. Nine “9” samples of undergraduate students actively enrolled in an undergraduate cybersecurity program in UAE universities were mindfully selected, and this truly reflects the broad group of the total population of undergraduate cybersecurity students in the UAE.

3.4 Research Experiment

In order to satisfy the objectives of this research work and provide true answers to its stated research questions, the experiment in this research work was devised in three distinct phases as elaborated below. It is important to note that due to the pandemic situation the entire research work, including the three phases of the experiment, was conducted online via Zoom, an online collaboration platform.

3.4.1 Phase 1 – Assessment Phase

This was the first phase of the devised experiment. The purpose of this phase was to understand and explore two crucial pieces of information from the selected 9 participants for this study. First and foremost, what was done was to understand the current hands-on technical skills that they have gained from their academic coursework. Secondly, their confidence level in approaching the cyber career industry to apply for a cybersecurity technical role was explored.

This assessment phase occurred in the first week that the participants were onboarded to this research experiment. The qualitative research instrument used for this phase was that of a one-on-one discussion session with each participant for one hour. During this hour, the two questions were asked, and the information shared by each participant was noted down by the researcher. The main aim of this phase was to understand the current state of assessment of the technical skills and confidence levels that these participants have before having access to the technical gamification simulation platform.

3.4.2 Phase 2 – Training Phase

This was the second phase of the devised experiment. The purpose of this phase was to provide the selected 9 participants access to the technical gamification simulation platform for 8 weeks. The technical gamification simulation platform consisted of two training platforms. One was the Cyber Range platform (CR) and the second was the Capture the Flag (CTF) platform. On the Cyber Range platform all participants had access to two different simulated real-world scenarios - one is related to digital forensics and the other is related to ICS/SCADA networking and incident response scenario. In the Capture the Flag training platform, all the participants had access to various technical cybersecurity challenges in domains such as digital forensics, web, cryptography, reverse engineering and OSINT. All information related to the completed technical scenarios and challenges by the participants was logged and noted down.

Due to the pandemic situation the training phase was also conducted online via Zoom. The participants were not required to attend the experiment at the premises. In addition, the training phase was conducted in a controlled environment. For example, all participants had equal access to both the training platforms (i.e., the cyber range platform and the capture the flag platform). This controlled environment enables a more exact measurement of participants' activity while maintaining the same setting for all of them. (Coolican, 2017) states when an experiment is performed in a controlled environment, the experiment becomes highly robust and trustworthy, especially when it is related to investigating and observing participants' cybersecurity-related behavior of problem-solving.

In addition, the technical gamification simulation platform provides the participants with hands-on technical experience in a simulated real-world environment. Consequently, this enabled a more precise assessment of the participants' talents and skills while maintaining the same conditions for all the participants. The participants can explore in a trial-and-error setting without putting themselves in a real-world situation, such as an organization's production network environment. Participants shall be able to use the technical gamification simulation platform whenever they want, wherever they are, whether at home or on the university's grounds.

Once the participants completed the 8-weeks period of having access to the technical gamification simulation platform a post-training assessment was conducted. The purpose of the post-training assessment was to capture the experience of the participants after having hands-on technical experience on the two training gamification simulation platforms. In this qualitative method the instrument used was an open-ended survey questionnaire (i.e., Google Forms) to allow the participants to respond to the questions based on their experience using the TGSP. All responses from the post-training assessment were logged by the researcher.

3.4.3 Phase 3 – Performance Phase

This was the third and final phase of the devised experiment. The purpose of this phase was to capture the scores of the participants from their hands-on technical skills experience via the technical gamification simulation platform. In this phase, the researcher developed a cybersecurity skills performance dashboard that displays the true assessment of the technical skills that a given participant has gained from the training phase. Through the dashboard any business owner can clearly identify which participants

are required to be interviewed to fill a vacancy that they may have by viewing the technical skills that they possess. Local security agencies can also use the dashboard as a national database for all cybersecurity talents and skills that are available in the country. The database can also be used as a reference for any participant to demonstrate their skills to any particular entity in order to be hired depending on their skills. The database will urge all cybersecurity professionals to continually update their technical skills so that their profile shows in the leader board of highly talented cybersecurity professionals. Furthermore, the policymakers can also refer to the dashboard to introduce new home-grown cybersecurity training and development programs to build cybersecurity capabilities depending on what skills are insufficient amongst the various cybersecurity professionals.

3.5 Technical Gamification Simulation Platform and Training Scenarios and Challenges

As stated above, technical scenarios and challenges were conducted on two different training platforms. In order to access the two different training platforms, the following was required. For the Cyber Range platform, it was a paid license; hence, the researcher purchased the licenses to create activated accounts for all the participants to have access to the CR platform. Appendix 2 exhibits a brief about the Project Ares Cyber Range Platform used for this experiment.

As for the Capture the Flag training platform, the training platform was available for free, and so the participants were only required to register with a username and password to have access to the platform. To access both the training platforms, the participants needed to have a good internet connection, a personal computer, and basic

knowledge of cybersecurity tools such as Kali Linux, IDA Pro, Oly Debug, Autopsy, Nmap, etc. Further details of the training platforms are mentioned below.

3.5.1 Cyber Range Platform – Battle Room 9: Digital Forensics

The science of detecting, gathering, maintaining, documenting, studying, analyzing, and presenting evidence from computers, networks, and other electronic devices are known as digital forensics (Bruce Nikkel, 2016). As technology becomes more integrated into our lives, the use of these technologies for criminal acts is more likely to occur, and this has necessitated the need for educational programs in the field of Digital Forensics not only in the UAE but around the world. As per Project Ares, battle rooms are scenarios that are designed to help assess the skills of the participants on a set of fundamental tasks specific to a topic. These scenarios are considered foundational building blocks that all cybersecurity professionals must be proficient at. These battle rooms are developed where participants need to execute it individually. The participants can either use the hints or decide not to use them to help with their learning experience. Once a participant joins a battle room, a simple network environment is presented with instructions and a list of tasks to complete. Appendix 3 exhibits a brief about Battle Room 9 and Mission 8. These were the two scenarios used in the experiment.

At the beginning of the 8 weeks experiment program, all participants had access first to the Cyber Range training platform. They were asked to complete Battle Room 9, a digital forensics scenario with 39 challenges that a participant needs to complete. Participants completed various tasks such as registry analysis, file system analysis, windows application analysis, online searches, and data analysis to locate relevant

evidence. Kali Linux, Autopsy, web inspection and USB historian are the most commonly used open-source tools for forensic tasks. The main steps involved in training are extraction of image files via different tools, analysis of data, finding evidence, and writing a report. Battle Room is further described in Appendix 3

3.5.2 Cyber Range Platform – Mission 8: ICS/SCADA, Networking and Incident

Response

The ultimate story on of SCADA attacks came out just over ten years ago. The Iranian Bushehr nuclear power plant was rendered inoperable by the Stuxnet malware. Stuxnet had infected around 50,000 distinct Windows' machines and 14 central control systems within a few months of the attack (GlobalData Thematic Research, 2021). Although this recent SCADA attack and a 2020 attack on a natural gas compressor facility aren't the same sizes as Stuxnet, they show that cyberattacks on manufacturing units and critical infrastructure are still a threat. The most recent incident emphasizes the need to improve the cybersecurity of water and wastewater facilities to match those of other critical infrastructure. Unhappy personnel should strengthen internal system management to avoid exploitation. Former US cybersecurity czar Christopher Krebs speculated that the attacker was "very likely" an insider, perhaps a disgruntled former employee with access to systems (GlobalData Thematic Research, 2021). As per Project Ares, missions are scenarios that are designed to assess the technical skill levels of the participants within a realistic simulated real-world environment. In the mission, the network environment presented to the participants is further complex than a battle room scenario and requires the participants to have multiple technical skill sets to complete the list of tasks. Once a participant joins a mission scenario, a complex network is presented,

mission orders and rules of engagement are listed and participants need to combine their multiple technical skills to complete the scenario. Further description of Mission 8 is provided in Appendix 3.

The second scenario that all the participants executed on the cyber range training platform was Mission 8, which is about the ICS/SCADA Networking and Incident Response scenario about responding to an attack in a water treatment plant. The controller of a treatment plant has been hacked in this scenario. The attacker gained root access to the SCADA and increased chlorine ten times greater than average. The contestants' main objectives are as follows:

- Identifying the adversary's IP address
- Restricting IP addresses from getting access to the network
- Verifying the SCADA process is normal and returning to normal mode
- Securing the control system by changing credentials and presuming policy controls

Kali Linux, Squid, Security Onion, Putty, and Nmap become helpful to participants. All the selected participants, that is, 3rd and 4th-year students, were able to complete both the scenarios on the cyber range training platform i.e., the Battle Room 9 and the Mission 8. Figure 2: depicts the Cyber Range Mission 8 as executed by a participant in the study.

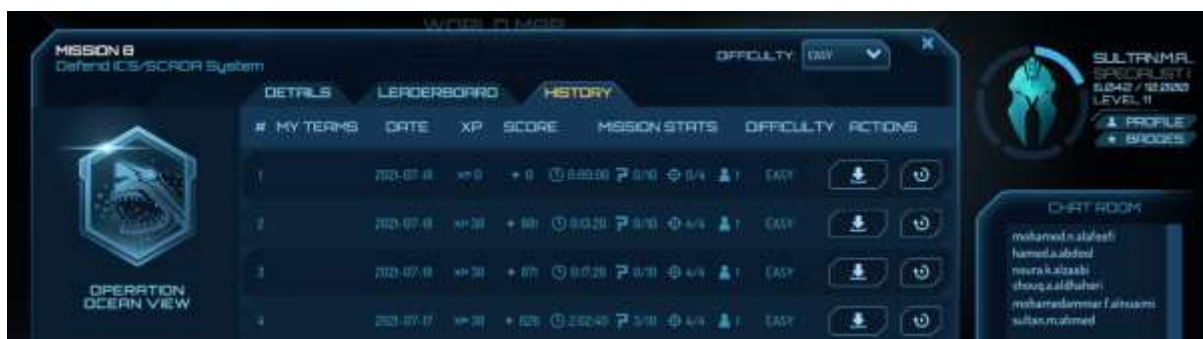


Figure 2: Cyber Range – Mission 8 scenario

3.6 Capture the Flag Platform

Capture the Flag is described as an online interactive training environment where the participants search for flags in any given technical challenges within the CTF platform (McDaniel, Talvi, Hay, 2016). The way the CTF works is once a participant finds the flag and the CTF scoring engine verifies it, the participant receives score/points for being able to complete a CTF technical challenge. In general, finding a flag provides clear evidence that the participant was able to demonstrate an adequate level of technical skills. Examples include accessing a file, exploring the registry, interacting with a service, etc.) Furthermore, CTF challenges evoke the adversary thinking skills in the participants. Hence, cybersecurity professionals can better understand the evolving cyber-attacks and eventually set up effective security defenses (Svabensky, Vykopal, Cermak, & Lastovicka, 2018). Every year the Telecommunications and Digital Regulatory Authority (TDRA) in the United Arab Emirates hosts CTFs to enable security professionals to test their technical skills either as individual participants or in teams. Even other big four technology firms such as Google and Facebook host CTFs (Google CTF, 2020) and (Facebook CTF, 2019). Capture the Flag are scenarios that are designed to assess participants' technical skill levels. Unlike the cyber range battle rooms and missions, capture the flag scenarios do not have any learning objectives and there are no hints or help that the participants can use to complete the scenario. Once the participant joins the scenario, an environment is presented, and the participants are required to use their existing technical skills to complete the stated challenge, whilst finding the hidden flags along the way.

In the 8-week long experiment duration, the participants were asked to access the CTF platform from the fourth week onwards until the end of the experiment duration. The CTF platform that they were asked to access was (<https://practice.ctf.ae/>). CTF.ae is based in Dubai, the United Arab Emirates. It creates and manages the CTF events and training with the aim of honing the technical skills of cybersecurity professionals. All participants were required to create their CTF accounts and start exploring and executing the technical challenges that are available on the CTF.ae platform. Various cybersecurity challenges were hosted on CTF.ae in different categories such as: digital forensics, web, OSINT, cryptography, PWN, and reverse engineering. The difficulty level of each of these technical challenges varied from beginner skills to intermediate skills and to advanced skills. Details of these categories are explored as follows.

3.6.1 Web Exploitation Attack

Numerous programming languages are used for web applications across the globe. Although there are distinct weaknesses in each computer language that perhaps the programmer ought to be mindful of, there are also many inherent problems to the web that can manifest independently of the tool or platform used. These flaws are frequently emphasized in CTF challenges. In other words, website security issues in which the user must exploit a flaw to achieve some form of increased level privilege is known as a Web CTF challenge. Participants followed various approaches to enable them find the flag in any given CTF challenge, as shown in Figure 3 below.

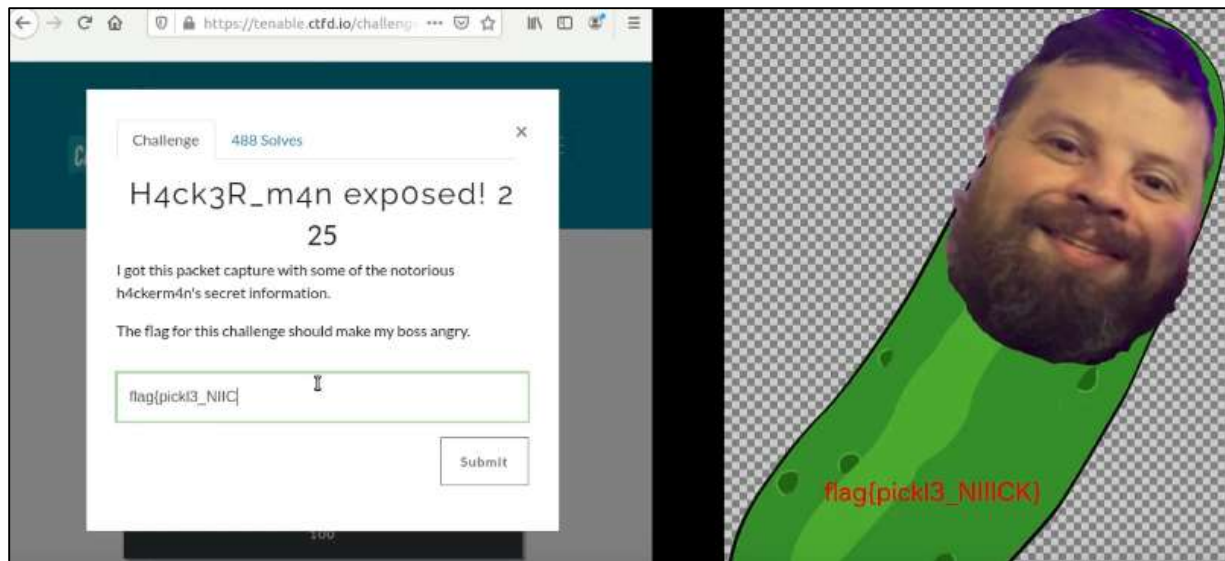


Figure 3: Example of capturing the flag in web-based training

The web challenges on CTF.ae enabled the participants to enhance their web exploitation technical skills such as cross-site scripting (XSS) attack to get the root-level privilege of the website. The main tools used in web exploitation were burp suite, python scripting to automate the process, and understanding of CSPs and security policies.

3.6.2 Reverse Engineering

Reverse engineering is a process of translating compiled code into a more human-comprehensible format. Object code is translated into assembly language using disassemblers. The main goals of disassembling a code are, comprehending a program, retrieving source code for archive or update purposes, identifying viruses, and troubleshooting programs. The main aim of reverse engineering training is to understand the functionality of the program such that the participants can identify more profound issues in the code. The tools used in executing the reverse engineering challenges on CTF were Ollydbg, IDAPro, to decompile the compiled code into code. (Chris Eagele, 2011) As shown in Figure 4.

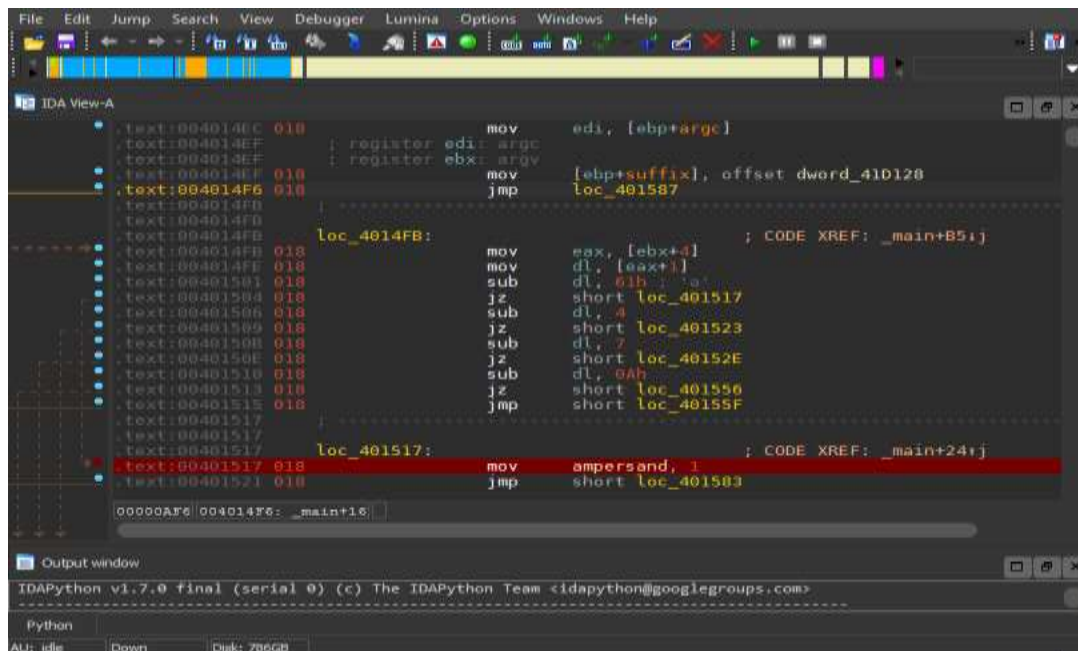


Figure 4: Decompiled code into pseudocode

3.6.3 Digital Forensics

Digital Forensics is the skill of retracing a desktop's digital trace. There are various techniques for locating evidence that appears to have been destroyed, not preserved, or, worse, secretly taped (Bruce Nikkel, 2016). Using the appropriate tools is a key aspect of digital forensics investigations. In this CTF digital forensics challenges, participants exhibited technical skills of being able to image the disk, extract and analyze the images, analyze the registry, and decrypt the password hashes. While executing the digital forensics CTF challenges, the main tools used were FTK imager, Autopsy, John the Ripper, and HashCat. Figure 5. Depicts digital forensics: L00k challenge executed by a participant.

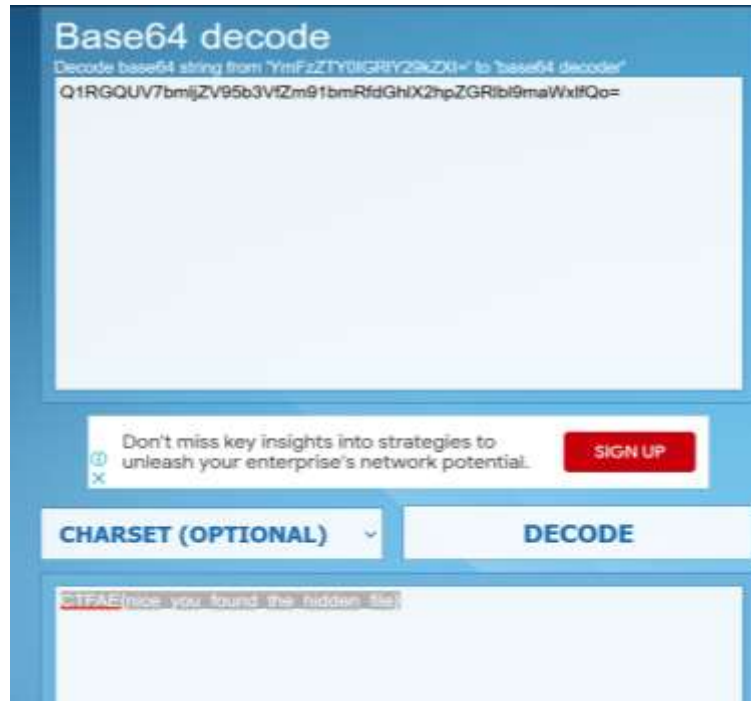


Figure 5: CTF Digital Forensics: L00k challenge

3.6.4 Open-Source Intelligence (OSINT)

The collection of data from public sources, including social networking sites, corporate websites, and news stories, is often known as open-source intelligence or OSINT. Via open-source intelligence, a wide variety of knowledge on an organization or individual can be acquired (Nicholas Crowder, 2015). The basic aim of the CTF OSINT challenges was to observe the approach the participants followed in order to collect the data and comprehend the fundamental clues concealed in the challenge mainly using Google search engine and some problem-solving and data mining abilities. Figure 6. Depicts the CTF OSINT Trail of 404s challenge as executed by a participant in the study.



Figure 6: CTF OSINT: Trail of 404s challenge

3.6.5 Cryptography

Securing business and transactions, private conversations, and safeguarding individual private data are just a few of the many security applications of cryptography (Douglas R, Maura B, 2018). To ensure the security of communications, cryptography is considered a vital component. The main aim of the cryptography CTF challenge was to ascertain the ability of the participants to break the encryption code that had been incorrectly implemented. The participants were required to develop a script in python to reverse the hash function. Figure 7. Depicts the CTF Cryptography Kyptonite challenge as executed by a participant in the study.

```
kali@kali: ~/Desktop/hashes.txt
File Actions Edit View Help
(kali@kali)~$ dcipher 50c9e8d5fc98727b4bbc93cf5d64a68db647f84
✓ D
(kali@kali)~$ dcipher 9f2059fa4172536236c9acfa22a911f918547e5
✓ DP
(kali@kali)~$ dcipher 8f720358b36c0ae92f1650ee09bb91f37d58422
✓ DPC
(kali@kali)~$ dcipher 48a688cc906642d86733f83595c7cac6eb520d3
✓ DPCT
(kali@kali)~$ dcipher 9fd2653434de8af111904bfbc9727b51171fddb
✓ DPCTF
(kali@kali)~$ dcipher 8f6109c5f17202f0ca0a9d53672a719d9c1aceb
✓ DPCTF[
(kali@kali)~$ dcipher 120da226f63a29013cc63c8423f221f0569ea18
✗ Hash could not be deciphered
```

Figure 7: CTF Cryptography: Kryptonite challenge

3.6.6 PWN

The "pwn" approach focused on exposing weak programs running on a remote server through the use of a remote script. In the CTF pwn challenge the participants were provided with a reverse engineering program as well as a server and port number. The server runs the same software and has access to the flag's data file (i.e., flag.txt). the participants had the ability to learn about secure coding (usually in C), through this challenge as a flaw in the code will allow the participant to reroute the program's flow (i.e., ability to find the flag). When it comes to penetration testing and exploiting codes, "pwn" abilities are deemed essential.

3.7 Scope of the Research Work

The focus of this research work was to demonstrate the enhancement of the hands-on technical skills amongst undergraduate students when having access to a technical gamification simulation platform. Hence, the scope of this study is limited to the shortage of skilled cybersecurity workforce in the United Arab Emirates. Work role guidelines of cybersecurity published by aeCERT and ADDA both security regulatory authorities of the United Arab Emirates state the job duties, eligibility criteria, and skill set required by each cybersecurity professionals related to a specific domain. Hence, this research work used the ADDA work role guidelines as the benchmark to rate the technical skills gained by the participants during their hands-on experiment on the technical gamification simulation platform.

All 3rd and 4th-year undergraduate participants (male and female) were enrolled in an eight-week experiment program and had equal access to both the training platforms. Various scenarios related to the Cyber Range platform and challenges related to the Capture the Flag platform were assigned to the participants in the form of tasks. Researcher had a close observation through the administrative panel to ensure that the participants worked on all the scenarios and challenges assigned to them. In addition, participants' performance was monitored via an administrative panel. Appendix 4 exhibits the 8-weeks program calendar layout for the experiment.

3.8 Data Collection

(Creswell & Creswell, 2018) have noted that in qualitative research method, data is collected to learn from the participants in the study. This is accomplished by developing forms, called protocols, to record data and the study progress. There are several forms

of collecting data from the participants in the study, such as an interview protocol where the researcher asks the participants in the study 4 to 5 questions or an observational protocol where the researcher records notes about the behavior of the participants. In the entire qualitative research process, the researcher tends to collect as much detailed data as possible and this enables the researcher to learn from participants through exploration (Creswell & Creswell, 2018)

In this research work, data was collected in various forms from the participants in the study and in different phases as laid out previously. Hence, the following list elaborates how data was collected and at what time intervals during the experiment program.

1. At the initial interview phase of selecting the participant for the experiment study, the data was recorded to understand the background of the undergraduate student and this included their academic skills, soft skills and technical skills. This data was recorded by the researcher in notes.
2. At the assessment phase, which is the first phase after onboarding the participants to the experiment program, data were collected through a one-on-one interview that lasted for an hour through Zoom. The aim of this interview was to understand the current state of assessment of the participants' technical skills and their confidence level to apply for a hands-on technical career once they graduate which is following the experiment program. The data was recorded by the researcher in notes.

3. Next, once the participants completed phase two of the experiment program that is the train phase, the researcher scheduled 2 hours Zoom online session with all the participants in the study and shared with them a survey questionnaire that had open-ended questions to evaluate what technical skills, abilities, and knowledge the participants had gained after the 8-weeks experiment period. The survey questionnaire was developed using Google Forms and all responses from the participants were logged in Google and the researcher was able to extract the excel responses sheet from Google.
4. In addition, the researcher employed the think-aloud method during the experiment program. Here, the participants in the study were asked to share their thoughts, ideas and experiences while they were executing the scenarios and challenges. The researcher created a WhatsApp messaging group and included all the participants in the study in the group so as to enable them to share their thoughts, experiences, views, and judgements, whenever they have one to share.
5. Furthermore, the researcher requested all the participants to provide regular reports of their experiences as being part of the experiment program and having access to the TGSP on both platforms. So, there were two reports shared by participants. The first one included sharing their experience after having technical hands-on access to Battle Room 9 and the CTF challenges. The second one included them sharing their experiences after having technical hands-on access to the cyber range Mission 8 scenario.
6. Moreover, once the experiment program was over, every participant, via a short interview was asked which platform they found useful more than the other in

comparison to cyber range and the capture the flag. Responses from all the participants were logged and noted by the researcher in notes.

7. Finally, all participants were requested to present on the lesson learned, and hands-on technical skills learned during the 8-week experiment program. Presentations from the participants were shared by the researcher and logged in the researcher participant experience database.

Throughout the experiment program the researcher was able to record a highly rich set of participant experience from the 8-week long experiment program. By gathering the data in the researcher participant experience database, it was evident that the repetitive affirmation provided as responses and experiences shared by the participants provided truthful assessment and view of the hands-on technical skills acquired by the participants in the study during this 8-week experiment program. Once the data was recorded, observed, noted and logged by the researcher then the process started as regards to cleaning the data and analyzing the apparent outcome.

3.8.1 Data Collection through Survey Interviews

(Creswell & Guetterman, 2019) stated there are many forms of surveys. Typically, researchers collect data using two basic forms: questionnaires and interviews. The researcher used these two forms of survey to collect the data for this study. Also, the researcher ensured to record the data whilst any of these forms of surveys were used throughout the study. An interview, as defined by (Creswell & Guestterman, 2019), is a form in which the researcher records answers provided by the participants in the study. The researcher asks the question from the interview guide, listens for answers or

observes behaviour, and records responses on the survey. In this qualitative study, the researcher used the one-on-one interviews as a form of survey data collection. The researcher selected this form of survey at the assessment phase of the experiment program to enable that the participants in the study share their views and experiences in a one-on-one setup without being influenced by other participants.

3.8.2 Data Collection through Survey Questionnaire

A questionnaire, on the other hand, as defined by (Creswell & Guetterman, 2019), is a form used in a survey design that participants in a study complete and return to the researcher. The participant chooses answers to questions and provides responses to questions asked. Mailed questionnaire is a form of data collection in survey research in which the investigator mails a questionnaire to participants in the study (Creswell & Guetterman, 2019). In this research study, the researcher used the mailed questionnaire form at the post training phase of the experiment program. The purpose of the questionnaire was to capture the experiences of the participants in the study about the use of the technical gamification simulation platform and to explore and understand the acquired hands-on technical skills and experiences of the participants.

The survey questionnaire started with informed consent, by ensuring that the participants of the study have the complete right to either provide their experiences and responses or decide not to progress. Once the participant decides to proceed with answering the questions, another note was made by the researcher urging the participant to answer all questions honestly, truthfully and accurately as much as possible in order for the researcher to collect as truthful and honest responses as possible. Then, the researcher went about listing the questions in the questionnaire. The researcher was

mindful and understood that most individuals do not desire to spend much time responding to questions and lose interest if the survey questionnaire is too lengthy. As a results, the questions were mindfully crafted. The researcher had a set belief that the responses of the participants might differ depending on their mindset, view, judgement and experience. Moreover, the survey questionnaire was developed not to include queries that are no longer in use or accessed independently. The researcher ensured that the participant is capable of answering all the questions in the questionnaire based on their experience within every phase of the experiment. As the researcher understands that if a tough or complex question is asked, it is doubtful that an honest and accurate answer will be provided by the participant and this is the kind of data that the researcher avoided.

The post-training survey questionnaire was sent to each participant via email on the day the online Zoom session was scheduled to enable the participants to have direct access to the questionnaire link once the zoom session starts. The ultimate purpose of the questionnaire was to assess and measure the effectiveness of using the technical gamification simulation platforms (TGSP) to upscale the hands-on technical skills of the participants in the study. The survey questionnaire can be found in Appendix 6.

3.8.3 Data Collection through think-aloud approach

The think-aloud approach is a research method in which the participants in the study can speak out loud and share their thoughts, views, experiences, ideas, and their minds as they undergo a certain task or experiment (Charters, 2003). It is a strategy that yields a large level of accomplishment rapidly by employing a qualitative measure (Leighton, Jacqueline P, 2017). Think-aloud method can be effectively interpreted

through qualitative research (Charters, 2003). The amount of qualitative information is considered to be rich can be collected from a limited number of participants taking part in a given experiment.

The researcher used this approach to be able to capture the thoughts and experiences of the participants in the study and when they have one to share when they are in action executing any given scenario and challenge. This form of urging the participants to share provides on-spot rich data that can add invaluable information to the overall research study. Through these real-time responses shared and other data collected throughout the experiment program, the researcher ensured that there exists no point in time where the data from the participants was not captured. Having a holistic approach to capture the responses from the participants during the experiment program provides truthful validity and certainty to test the research questions set for this research work. As (Creswell & Creswell, 2018), noted qualitative research reports contain extensive data collection to convey the complexity of the process. In reporting qualitative research, a wide range of formats are used to give a report on the findings, hence, convincing the reader that the study is accurate and of credible account (Creswell & Creswell, 2018).

3.9 Data Analysis

(Creswell & Guetterman, 2019) stated that analyzing qualitative data requires the researcher to understand how to interpret and make sense of the text and images so that as to form answers to the research questions. Qualitative data is typically gathered in a text database so that the data analysis of this text consists of dividing it into groups of sentences, known as *text* segments and determining the meaning of each group of

sentences (Creswell & Guetterman, 2019). In a qualitative research method, words are analyzed to describe the central phenomenon that is under study, which in our case to understand and explore the enhancement in the hands-on technical skills of the participants of the study.

3.9.1. Data Cleaning

This first step towards data analysis is data cleaning to ensure that no information has a missing value or an outlier. For this research work, data cleaning was conducted through manual screening of going through the extensive data collected preserving them in the participants' experience database. The researcher wanted to ensure higher reliability score of data collected, hence, screened the data to flag out any missing data or removed any response given by participants that had missing fields. The main database included a total of 9 responses from a total of 9 participants in the study hence, all participants in the study agreed to respond to the questionnaire. All the 9 responses were finalized once data screening was completed. Once data cleaning was completed, reliability tests were conducted to ensure scoring consistency in the skills performance dashboard.

3.9.2. Data Organization and Preparation

Once the data cleaning step and ensuring its reliability was completed the next step was to ensure data is organized and prepared to be presented and validated against the set research questions for this research work. The data were organized within categories that will enable a better presentation of data collected, and having the researcher being extensively aware of the knowledge of this area helped with this step.

In addition, various data were organized in separate folders according to each participant of the study. Once data was organized and prepared, it was time to read the data to understand and ensure there is reliable, accurate and credible data that can be reported and this tests and validates the set research questions of this research work.

3.9.3. Data Coding

Creswell & Creswell (2018) categorized coding qualitative data into three categories. First, codes on areas that an observer shall expect the finding either based on past literature or common sense. Second, codes that are unusual and interesting findings to the observer. Finally, codes that are not expected as a finding. Hence, a code database was developed and it included the various codes, categories, descriptions and examples of quotes shared. This can be found elaborately in Appendix 7.

3.9.4. Qualitative Data Analysis

Once data was cleaned, validated, organized, prepared and coded, then, the final analysis part commenced. The research used both to hand analyze the data and to use a computer depending on the data collected. The researcher hand analyzed the data from the one-on-one interviews, reports submitted and the think-aloud form. The computer analysis of the data was used for the questionnaire responses. According to (Creswell & Guetterman, 2019), hand analysis of qualitative data refers to when the researcher reads the data, marks it by hand and divides it into parts. On the other hand, a computer analysis of qualitative data (QDA) refers to when the researcher uses qualitative software to facilitate the process of storing, analyzing, sorting, and representing or visualizing the data. The QDA software programs store data, organize it, enable the researcher to assign

labels or codes to the data and facilitate searching through the data to locate specific text or words of interest. The software used for this research study was MAXQDA. MAXQDA is a data analysis tool for text analysis used for grounded theory-oriented, code-and-retrieve analysis and more complex text analysis. Appendix XX includes screenshots of the qualitative data analyzed using MAXQDA.

Additionally, the three forms of data collected that were hand-analyzed by the researcher are as follows. The first form of data collected through the one-on-one interviews that were conducted at the assessment phase of the experiment program was hand-analyzed. The second form of data collected that were from the administrative panel of the two training gamification platforms that is the cyber range and the capture the flag, were also hand-analyzed. Finally, the data collected from all the observations made by the researcher in relation to the participants in the study, in addition to the think-aloud responses that were collected through the Whatsapp group were also hand-analyzed.

In addition, the use of open, axial and selective coding was used to analyze the data (Strauss & Corbin, 1998). For the open coding, each text transcript was hand-analyzed in sentences reflecting the participants' experiences. These units were provided a code to reflect an idea or concept (Strauss & Corbin, 1998). There were 200 items identified through open coding that were combined using axial coding to 10 abstract concepts. When using selective coding the concepts were organized into a central category. In this study, it was the technical gamification simulation platform along with five categories: 1. Digital forensics, 2. Cryptography, 3. Network Security and Incident Response, 4. Reverse Engineering and 5. Web Security. Attributes for each of these categories were also identified. Through constant comparative analysis (Strauss &

Corbin, 1998), each participant's response was compared and linked to other participants as the categories and properties emerged.

3.10 Validity and Reliability

According to (Wellington, 2015), reliability refers to the ability to which a technique, test, or research instrument currently measures what it purports to measure. In contrast, reliability refers to both the extent to which an instrument, technique, or tool produces reliable results along with a range of locations and when used by a variety of researchers. In addition, according to (Creswell & Geuttermann, 2019), validity refers to the development of sound evidence to demonstrate that the intended test interpretation matches the proposed purpose of the test. The researcher in this research work tested the collected data from all the participants of the study and ensured the validity and reliability of the research instruments for this study. Additionally, the researcher regularly asked for expert assistance from the supervisor to ensure that the method and approach followed to collect and conduct the research is valid and reliable.

3.11 Ethical Consideration

This research work was conducted with complete guarantee that the participants are willing to take part in this 8-week long experiment program. The participants had complete freedom to respond to a certain question or execute a certain scenario or challenge. The researcher ensured that at all times, all data collected from the participants were honest, accurate, and credible. Core ethical principles were examined, ensuring the privacy and protection of research participants' identity, while all participants did not mind if their identity is revealed for this research purpose. In addition, before commencing the

research experiment, the researcher ensured that the participants of the study gave their informed consent of being a part of this research work.

3.12 Summary

In conclusion, this chapter provided a detailed explanation of the research method and design used for this research work. The chapter started with presenting the research method and design employed by the researcher in this research work. Then, the target population and participant selection criteria were explained. The researcher then expanded upon the three distinct phases of the experiment. An outline and description of the two training technical platforms were presented, including the scenarios and challenges that the participants had access to. Then, an inclusive description of data collection methods and processes was elaborated on. Finally, a description of the data analysis procedures was presented. The next chapter, chapter 4 discusses the results obtained from the various data collection methods for this qualitative grounded theory research in detail.

Chapter 4: HANDS ON EXPERIMENT RESULTS

This qualitative grounded theory study examined whether the use of a technical gamification simulation platform alongside the cybersecurity academic program would raise the hands-on technical skills of undergraduate students. This chapter presents the outcomes of the qualitative data analysis. The standard online survey tool, Google Forms, was used to collect the responses of the participants in the study while using an account owned by the researcher. All the responses of the participants were exported from Google Forms into an excel format and appropriate data cleaning, organization, and preparation mechanisms were applied to the data to make it easily readable for the researcher.

The experiences, insights, views, and reflections shared by the participants in this study revealed the dynamic process of introducing the use of a technical gamification simulation platform alongside the cybersecurity undergraduate academic program. This was because it was explored through a process of sequence of activities, actions and interactions among the participants during the experiment program (Corbin & Strauss, 2015). The grounded theorist examined the participants (e.g., through interviews, observations, and questionnaires) and an understanding of the process of technical skills being enhanced gradually emerges. The researcher categorized this information by drawing evidence to support each category and this is known as the open coding phase. Then, the researcher organized the categories into a model and this is known as the axial coding. Finally, the researcher interrelated the categories to form a theory that elaborates the process of upscaling the hands-on technical skills.

The researcher collected many forms of qualitative information to establish the above explained processes. Such collected data include observations, conversations, interviews, and questionnaires, and the researcher's own personal reflection (Charmaz, 2000). The procedure used to collect the data followed an emerging design, and this means that the researcher collects initial data, analyzes the data immediately for preliminary categories and then looks for signs and decides on what additional data needs to be collected. Hence, the entire procedure followed was that of a zigzag data collection and analysis until saturation of categories is achieved. In other words, the researcher continues collecting data and analyzing until a decision is made in a way that any further new data collected will not provide any new information or insight for the developing categories.

The analysis of the qualitative data was conducted in two phases. The first phase included analyzing the participants' responses to the survey questionnaire using a qualitative data analysis software known as MAXQDA. The second phase was analyzing the scores that the participants received as part of the completion of the various scenarios and challenges on both the cyber range and capture the flag platforms. The responses of participants to the survey questionnaire items were analyzed to determine the percentages of the agreement through the in-built analysis tool in the survey platform (Google Forms). Appendix 6 presents the Google Form questionnaire that was distributed to all the participants. Appendix 7 exhibits the responses received from all the 9 participants of the experiment in response to the post train phase questionnaire.

This analysis presented the percentage values and the number of participants who agreed with the statements in the items that included multiple-choice type of questions.

The second phase of the analysis involved analyzing the statements entered by participants for the open-ended questions on the survey. The analysis of these statements adopted a qualitative content analysis strategy which refers to "...a systematic coding and categorizing approach used for exploring large amounts of textual information unobtrusively to determine trends and patterns of words used, their frequency, their relationships, and the structures and discourses of communication" (Vaismoradi et al., 2013).

In line with the suggestions of Mayring (2004), the analysis started with inductive category development based on an analytical interpretation of the content of the questions that required participants to submit written responses. Next, the responses of participants were read several times to ensure their connection with these categories to perform deductive category application. In this stage, the coding rules were also settled to determine exactly under what circumstances a text passage can be coded with a category. Lastly, the text was coded based on the code rules, and the codes were grouped under relevant categories.

As for the second mode of analysis, responses were extracted from the administrative panel of both the cyber range and capture the flag platform. The researcher had administrator access rights to both the training platforms in order to extract the information about each of the participants in the study are regards to the scores achieved in each of the scenarios and challenges completed, the number of times the participant played a scenario on the cyber range platform, the time spent playing a scenario on the cyber range platform, etc. The researcher cleaned this data, organized and prepared it. In order to help visualize the performance of each of the participants and present how the

TGSP raised the hands-on technical skills of the participants, the researcher designed and developed a cybersecurity skills performance dashboard to provide a visual presentation of the participant's technical proficiency level.

4.1 Responses from the One-on-One Interview Questions

As mentioned previously the experiment program had three phases viz assess, train and perform. In the first phase of the experiment, that is, the assessment phase, a one-on-one interview was conducted with each participant in the study in order to understand the current level of technical skills that each participant has. After starting the interview with an opening question to learn more about the participant and build the connection. There were three questions asked as follows:

4.1.1 Assess: Current Technical Skills

The first open-ended question asked was, *“On a rate of 1-5, where 1 is my technical skills are minimal or being developed and 5 is advanced technical skills, how do you rate your current hands-on technical skills gained from the university?”* 7 out of the 9 participants in the study shared the same view that *“I do not know what technical skills I currently have as the focus at university is theoretical more than practical and even if we are provided technical assignments to complete, these are extremely basic and do not reflect the real-world environment”* and the remaining 2 participants answered, *“1, being developed, maybe.”* The researcher noted down the answers to the first question.

4.1.2 Assess: Current Confidence Level

The second open-ended question that was asked following the first one was, *“On a rate of 1-5 where 1 is least confident and 5 is most confident, how you rate your*

confidence level in applying for a technical cybersecurity role once you graduate?” 9 out of the 9 participants in the study had the same answer of “1, least confident to apply for a technical role at this stage as I believe I am not ready to provide any hands-on technical skills.”

4.1.3 Assess: Usage of Gamification Platform at University

The third open-ended question that was asked following the second one was, *“Have you used any of the gamification platforms at your university in order to build your technical skills, such as a cyber-range or capture the flag platform?”* 7 out of the 9 participants in the study had no idea about both platforms that is the cyber range and capture the flag platform. 2 out of the 9 participants did participate in capture the flag competition as contestant part of the team. 6 out of the 9 participants added to mention that they have attended an ethical hacking course at university. This last experience added by the participants was interesting to know because it showed that all the 9 participants who passed the selection interview only did because they had the required foundational cybersecurity knowledge and basic technical skills from either attending the ethical hacking course or from being part of the capture the flag event. The reason for this observation was because both of these events provided the participants with a simulated real-world environment to assess their technical skills using real-world tools.

4.1.4 Purpose of Assessment Phase

The assessment phase interview’s purpose was to gauge the current technical skills state and assess the confidence level amongst the participants in the study for these responses to serve as the basis for further comparative analysis with post-training

assessment responses. This will enable the researcher to provide a clear measure of enhancement of the participants once they have used the TGSP.

4.2 Responses from the Post-Training Questionnaire

This qualitative grounded theory research study aims to understand and explore how using a technical gamification simulation platform may enhance the hands-on technical skills of undergraduate students who majored in cybersecurity. The qualitative data collected to this end inquired the relevant experiences, insights, and views of the participants in the study during a structured experiment program that lasted for eight weeks. During the experiment program, the participants conducted several experiments on two gamification platforms (Cyber Range (CR) and Capture the Flag (CTF)). All participants were provided with access to the training platforms at the same instant and the structure of provisioning the access of the experiment was as follows:

1. Access to Cyber Range – Battle Room 9 scenario: This is a basic foundational scenario. It expected that any cybersecurity proficient must have basic technical skills to execute it.
2. Access to Capture the Flag – Several different scenarios: Various difficulty level scenarios are presented to participants to use their existing skills to complete the scenario by finding the hidden flag.
3. Access to Cyber Range – Mission 8 scenario: A complex network scenario that assesses the advanced technical skills of a cybersecurity professional within a simulated real-world environment.

The experiment program was structured to presenting to the participants basic scenarios to complex scenarios to ensure a gradual learning process for the participants and data was collected and analyzed at every phase of the experiment. The analysis of a qualitative survey questionnaire was administered after the end of the experiment program and revealed that the participants were able to construct new hands-on technical skills, knowledge, and abilities in all of the domains addressed within the learning objectives of the experiment program. Figure 8 depicts the responses from the participants in regards to the Informed Consent of them being willing to participate in the post-training phase questionnaire.

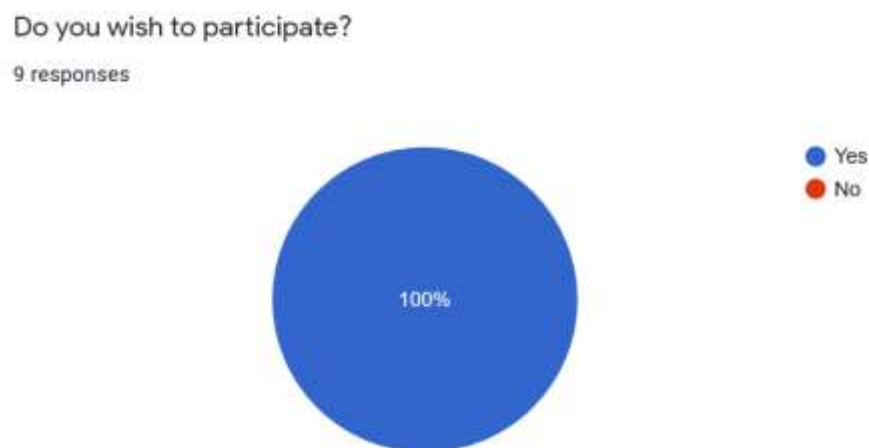


Figure 8: Informed Consent of Participants as Response to Post-Training Questionnaire

4.2.1 Post Train: Knowledge Gained

In terms of participants' responses related to knowledge gained, all of the participants in the study could acquire knowledge related to *the investigation, auditing, and forensics methods, processes, procedures, and standards, and the concepts and practices of processing digital forensic data*. As depicted in Figure 9.

2) The knowledge I gained by attending these lectures are the following: (Select all that applies)

9 responses

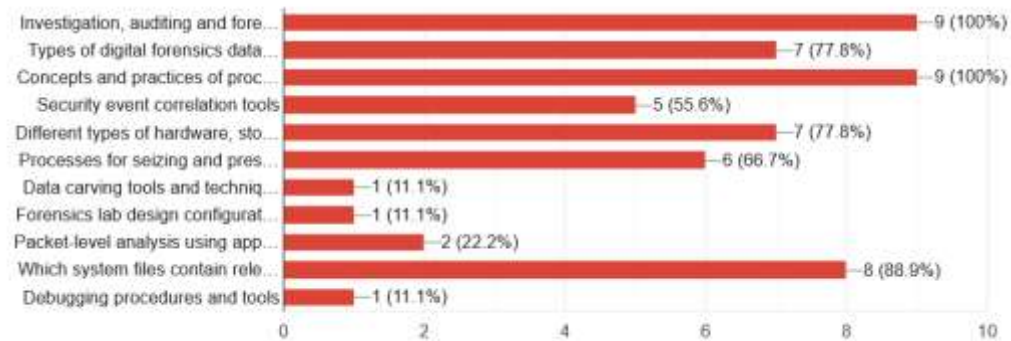


Figure 9: Knowledge gained from the experiment stretched the 8 weeks

Also, the majority of the participants were able to improve their knowledge in terms of *which system files contain relevant information and where to find those system files* ($n = 8$), *the types of digital forensics data and how to recognize them* ($n = 7$), *different types of hardware, storage, imaging and file system analysis* ($n = 7$), *processes for seizing and preserving digital evidence* ($n = 6$), and *security event correlation tools* ($n = 5$). Nevertheless, the number of participants who were able to acquire new knowledge in the domains of *packet-level analysis using appropriate tools* ($n = 2$), *data carving tools and techniques* ($n = 1$), and *forensics lab design configuration and support applications* ($n = 1$) was relatively lower. The reason why the last three findings were low is that because these were considered advanced level knowledge that required the participants to have hands-on experience on additional complication scenarios to build that knowledge.

The participants were also asked an open-ended question about what further knowledge domains in which they were able to construct new knowledge after attending the training program. According to participants, they got more familiar with and competent

at some concepts, including *the stages of the attack lifecycle, choosing appropriate tools for forensic analysis, the types of threats and their threat actors, different phases and requirements involved in the investigative process, and digital forensics enforcement challenges at the international level*. Figure 10 depicts partial sample of the responses from the participants.

3) Kindly elaborate what other knowledge have you gained more than the ones mentioned above.

9 responses

enforcement challenges, The stages of the attack lifecycle, The responsibilities of forensic investigators, and the current cyber threat landscape.

Different network tools like firewalls, IDS, IPS.

general information about different areas of cybersecurity.

logs on hardware equipments like firewall and switches, difference of digital and network forensics, types of antiviruses used in enterprises, actors/attackers categorizes, nation and non nation actors procedures, types of IDS : misuse and anomaly.

the attack lifecycle

- I have learned how to think as an investigator, where to look for evidence, and what kind of evidence to expect to find. Also keeping in mind the criminal mindset to think like a criminal to discover traces that could lead understanding how a certain attack was delivered.

revised enterprise network devices and services

Figure 10: Responses from participants on the open-ended question about additional knowledge gained

4.2.2 Post Train: Skills Gained – Cyber Range

The survey also inquired about the experiences of participants with the Battle Room 9 of the Cyber Range platform to which they all had access for eight weeks. While working on this platform, the participants were able to experiment with Battle Room 9

which includes various challenges touching upon a diverse range of issues within computer forensics.

According to the responses of the participants, the benefits of the Cyber Range platform were most visible on *identifying and extracting data of forensic interest in diverse media* (n = 8). The other hands-on skills that the participants were commonly able to develop after attending the training program included *analyzing memory dumps to extract information* (n = 7) and *using forensic tool suites (e.g., EnCase, Sleuthkit, FTK)* (n = 6). Nonetheless, only a minority of participants were able to record self-perceived progress in terms of *system administration skills for different OS (Windows, UNIX, Linux, Mac OS, Exchange, etc.)* (n = 4), *preserving evidence integrity according to standard operating procedures* (n = 4), *processing digital evidence to include protecting sound copies of evidence* (n = 3), *interpreting results of the debugger to ascertain tactics, techniques, and procedures* (n = 2), *programming skills such as C, C++, Java and others* (n = 1), *analyzing anomalous code as malicious or benign* (n = 1), and *conducting forensic analyses in multiple operating system environments* (n = 1). Figure 11 depicts the responses of the participants on the same.

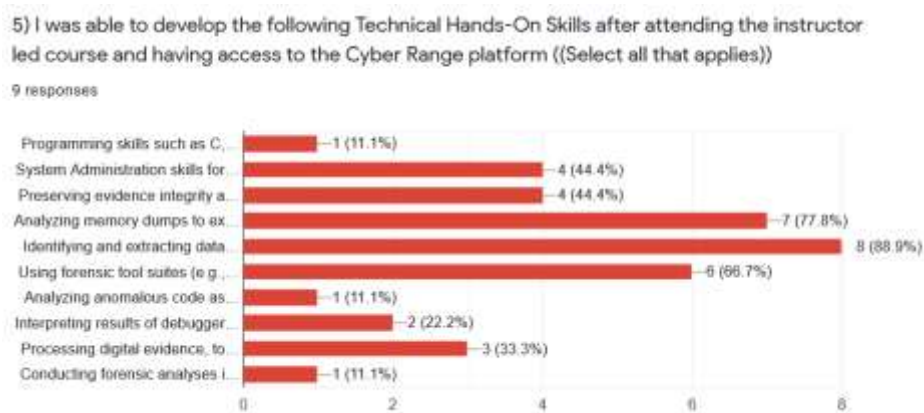


Figure 11: Participants responses on the Cyber Range platform

In addition to these domains, the participants responded to an open-ended question about any additional technical skills that they have gained. These additional hands-on technical skills were in the field of digital forensics, in which the participants were referred to a total of 28 skills, including using new tools that they had not been able to experiment with before the program. These tools included Autopsy (to obtain data from the client's computer, recover browsing histories, analyze the traffic on e-mail clients), Ophcrack (to crack Windows passwords), and Registry Explorer (to analyze system hives). Figure 12 presents the partial sample of the participants response to the open-ended question in regards to the additional technical skills that they have gained other than those that were listed.

6) Kindly elaborate what other technical hands on skills have you developed more than the ones mentioned above from Battle Room 9.

9 responses

i used tools i never did before:
how and where to look for certain type of information

hashes type, attention to details, forensic tools advantages and how they work, recognizing different type of files like deleted files and root files, cracking password using a forensic tool.

We have used Autopsy.

- I learned how to use Autopsy (A collection of tools grouped into a GUI app) an open source and a very powerful and useful tools in forensics.
- I learned how to analyze an email client, recover messages sent, attachments - (Autopsy)
- I learned how to use Autopsy to recover browsing history (even the deleted ones) - (Autopsy).
- I learned how to browse through registry using various tools such as Registry explorer, such tools makes it easier to understand data within the registry and track changes made on an windows based operating system such as installed applications, removed applications, user-registration info and operating system installation date.

Learned how to use different tools such as Autopsy and Registry explorer

Figure 12: Participants responses to the open-ended question in regards to the additional skills learnt

Other hands-on technical skills they acquired using the cyber range platform were mentioned and it relates to how and where to look for a particular type of information, analyzing data in different parts of a device, understanding artifacts of execution and where to locate them, and navigating the Windows NTFS file system and the registry structure. Another area was network security and incident response, in which the participants mentioned skills such as configuring and verifying IDS SNORT rules to alert the monitoring center on suspicious traffic and creating, modifying and deleting firewall rules utilizing firewallID as a firewall management tool, utilizing the command-line environment (BASH) to perform tasks where needed, and monitoring network events and identifying security incidents with Security Onion through both Squil and Squert.

The third area was related to web security. In this field, the students could realize gains as they became able to understand CSPs, content security policies, and the ability to bypass them to pull off cross-site scripting XSS attacks, use Python programming more efficiently to create scripts and speed up specific tasks, and use the built-in “Inspect Element” option in browsers. One other area of additional gains was reverse engineering, and the participants argued that, as a result of their practicing in the Cyber Range platform, they enhanced their competencies in terms of using disassemblers (Binary Ninja) and debuggers (Ollydbg and gdb) for static and dynamic analysis and using new tools such as IDA. The final area was cryptography in which the gains were listed as decrypting an emoji-based encrypted message and developing python scripts to reverse hash functions.

4.2.3 Post Train: Skills Gained – Capture the Flag

Within the training program, the participants also worked on the capture the flag platform, in which the participants were required to work on and successfully execute a number of challenges. While all participants stated their satisfaction with the cyber range platform, the satisfaction rate dropped to **67%** with the capture the flag platform. The analysis revealed that the challenges that were the most frequently worked on included L00K (n = 8), Keep It Simple (n = 8), Trails of 404s (n = 7), Keep Searching (n = 6), Awesome (n = 5), and Super Password (n = 2). The participants stated that executing the challenges in the CTF platform enabled them to build additional hands-on technical skills and further improve other existent technical skills that they have. The most commonly mentioned skills included *using new tools (e.g., John the Ripper, Phyton scripts, etc.) to decode hashes* (n = 7), *working with hidden files* (n = 3), *performing dictionary attacks using John the Ripper* (n = 3), and *using web proxies to deliver web-based attacks* (n = 2). Figure 15 depicts the responses from the participants to the value brought in by the CTF platform.

3) What technical hands on skills have you gained by working on Capture the Flag platform? Kindly elaborate

9 responses

Developing a python script to reverse a hash, Discover hidden files within a ZIP file, enforced my skill in performing dictionary attack using john the ripper, enforced my skill in using web proxies to deliver web-based attacks, Enforced my programming skills, discovered the importance of OSINT.

While working on the CTF platform, I gained many skills while attempting some of the challenges. These include knowledge and experience using different (some new) tools to tackle some of the challenges, such as disassemblers for the reverse engineering challenges, and password/hash cracking software for the digital forensics and cryptography challenges.

Its a long list, but honestly every challenge I've performed helped me learn something new within its category.

Web Challenges:

- Better Utilize Burp Suite
- Analyze POST/GET HTTP requests.
- Utilize Python to speed up manual tasks.
- Better utilize SQLMap to pull off SQL injection attacks.
- Understand the concepts of content security policies (CSP), and how they work as protection against XSS.

Figure 13: Participants' responses to the skills gained working on CTF platform

Similar to the cyber range platform, the capture the flag platform was also considered to be an invaluable testing platform for the participants in the study and one that they could continue to use in the future to further improve their technical skills. The most commonly referred to reason for this experience included the exploration opportunities as the participants experimented with different tools at their convenience:

While working on the capture the flag platform, I gained many skills while working on some of the challenges. This includes knowledge and experience using different and new tools to tackle some of the challenges, such as disassemblers for the reverse engineering challenges and password/hash cracking software for the digital forensics and cryptography challenges. (Participant 7)

The participants also believed that the capture the flag platform was both useful and enjoyable, and this allowed them to entertain themselves while improving their practical

and professional technical skills and knowledge. Finally, some participants argued that the capture the flag platform was invaluable in the sense that it gave them a chance to verify the extent to which the information they were exposed to in their courses helped solve simulated real-world problems.

4.2.4 Post Train: Confidence Level

All participants agreed that they became more confident with their hands-on technical skills and their capability to solve real-world environment cybersecurity incidents as a result of working on the challenges on the cyber range platform for eight weeks. Figure 13 depicts the participants' response about their confidence level in their hands-on technical skills after being exposed to the TGSP. Most of the participants stated that they were overly satisfied with the learnings from the cyber range platform as they benefitted both theoretically and technically.

5) Are you more confident of your technical skills as you keep working on challenges on Capture the Flag platform?

9 responses

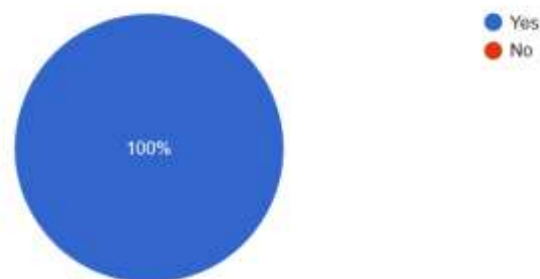


Figure 14: Participants' responses in regards to their confidence level of their technical skills while working on TGSP

In this context, six participants argued that the most outstanding contribution of the cyber range platform was that it helped them build what they had learned at school. For example, Participant 7 argued that he would like to continue using the cyber range platform even after the training period and explained his reason as follows: *“This is because the cyber range platform has been a very useful tool for me to further my learning at the university and better understand the field of digital forensics.”* Another benefit of the cyber range platform that the participants equally appreciated is that they were able to link their theoretical understandings with practical applications, which helped them become more familiar with real-world professional practice. In this context, Participant 8 argued that the training program gave her valuable opportunities in applying her knowledge in real-life situations:

I believe that the exercises at the university are very basic and do not reflect real-life scenarios, but learning using the cyber range and capture the flag platforms will definitely give the students a better understanding of how to apply their theoretical knowledge. (Participant 8)

In addition, the participants believed that the cyber range platform gave them valuable ground on which they could improve their technical skills. More specifically, they stated that the platform enforced their technical skills by putting them to the test in which they were supposed to apply the academic and theoretical knowledge they had acquired in their courses to solve challenges from the real world of digital forensics. Figure 14 depicts the participants' responses in regards to value received from the TGSP and their willingness to continue using the platform to upscale their hands-on technical skills.

12) In your honest opinion, if you continued having access to a Cyber Range platform with wide variety of Battle Rooms and Missions will you continue using it to up scale your technical hands on skills while you are no more an undergraduate student? Kindly elaborate.

9 responses

Definitely yes, as explained in the previous question. These platforms helps me to identify my weakness and strength. In other words, it helps me on improving my weak points and even strengthen my strong points by discovering other ways to perform a certain task.

In the provided scenario, I would definitely continue using the Cyber Range [CR]. This is because the CR has been a very useful tool for me to further my learning and understand of the field of digital forensics. I believe that this extends to other fields of cybersecurity, and so would definitely continue practicing on the CR build further skills and sharpen existing ones in different areas of cybersecurity.

Yes I would. The format of the cyber range is more focused when compared to CTFs and the like, allowing us to become much more familiar with the tools used to reach an objective. (e.g. Battle Room 9 wanted to introduce Forensic Analysis with Autopsy as a main tool, and after doing it I feel much more comfortable with utilizing autopsy)

That and I also enjoy doing technical tasks such as those offered in the cyber range.

Yes I would continue using them as there are many various types of battle rooms and missions to explore and to gain skills from them to practice and crave many skills into me.

Figure 15: Participants responses on their continuation of the use of TGSP

Finally, one of the participants stated that the cyber range platform was also valuable in the sense that it created a community of practice for the participants in the experiment program where a group of like-minded people with similar interests came together to work towards the same goal. Considering the various benefits of the cyber range platform, the participants stated that they do have intentions to use it in the subsequent stages of their training. The most common reason why they wanted to continue using it was their belief that they could enhance their hands-on technical skills as they did more practice using the various scenarios offered by the platform. For example, one of the participants stated his reason as follows:

I believe that the benefits we had in this program might extend to other fields of cybersecurity, and so I would definitely continue practicing on the cyber range

platform to build further skills and sharpen existing ones in different areas of cybersecurity. (Participant 7)

Moreover, two participants shared that they found the cyber range platform to be more focused compared with other platforms with which they were familiar. For example, Participant 4 suggested that each battle room in the platform catered for a specific skill, which made it especially useful for users who aimed to improve their technical skills in specific areas. Lastly, all the participants shared that they would continue using the cyber range platform because it was more practical and enjoyable compared to its counterparts, and it helped them develop problem-solving skills and discover their weaknesses and strengths as regards the current hands-on technical skills that they have.

When asked about their experiences after completing the experiment program, all participants reported varying levels of self-development. Almost all participants stated that they acquired new skills in terms of *dealing with highly sensitive or confidential data or images* (n = 8), *presenting and explaining findings and reports when necessary to all interested parties* (n = 8), *having an analytical mind with the ability to respond quickly to findings* (n = 8), *decrypting digital data collections* (n = 7), *conducting forensic analyses in and for both Windows and Unix/Linux environments* (n = 7), and *keeping up to date with evolving cyber-crime methods and developments within the digital forensics field* (n = 7). In addition, the majority of participants stated that they showed vital signs of improvement in *determining how a computer was broken into* (n = 6) and *providing forensic support to Cyber Security Operations during the investigation of any detected threat or contained incident* (n = 5). There were also a small number of participants who indicated that they were able to gain new skills as they *reviewed detailed incident*

management reports based on incident investigations (n = 3) and used expertise in a corporate setting to protect computers from infiltration (n = 2). Figure 16 depicts the participants' responses to the same.

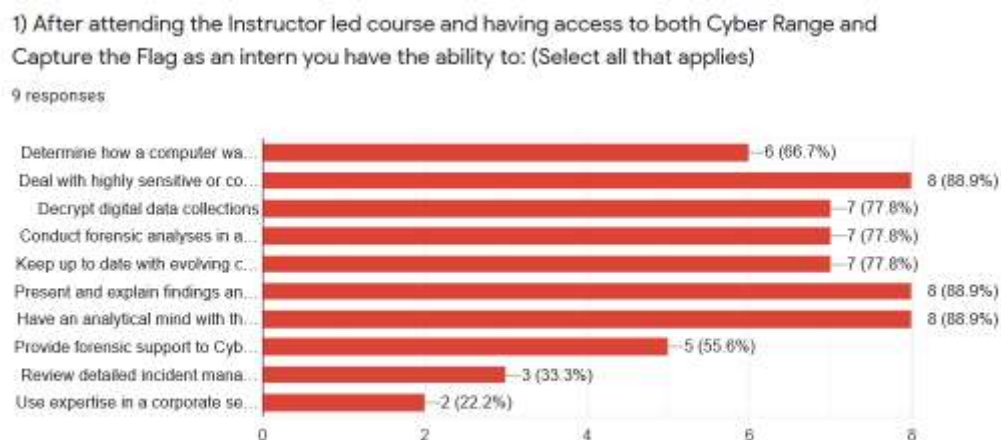


Figure 16: Participants' responses to the overall hands-on experience to both CR and CTF platforms

4.2.5 Post Train: Proficiency Level

As a result, **67%** of the participants reported their proficiency level in digital forensics at the intermediate level (Level 3) which entails the capability to demonstrate a working or functional proficiency level sufficient to apply the competency effectively without assistance and with minimal supervision as well as having functional knowledge of the subject matter area. The rest of the participants, that is **33%** believed that they were able to reach the basic level (Level 2) as a result of their participation in the training program which means that they were able to demonstrate a limited use of relevant competencies in the field of digital forensics as evidenced by having basic familiarity with the subject matter and needing additional training to apply with assistance or without

frequent supervision. Figure 17 provides participants' responses to their perception of their proficiency level after having hands-on experience on both CR and CTF platforms.

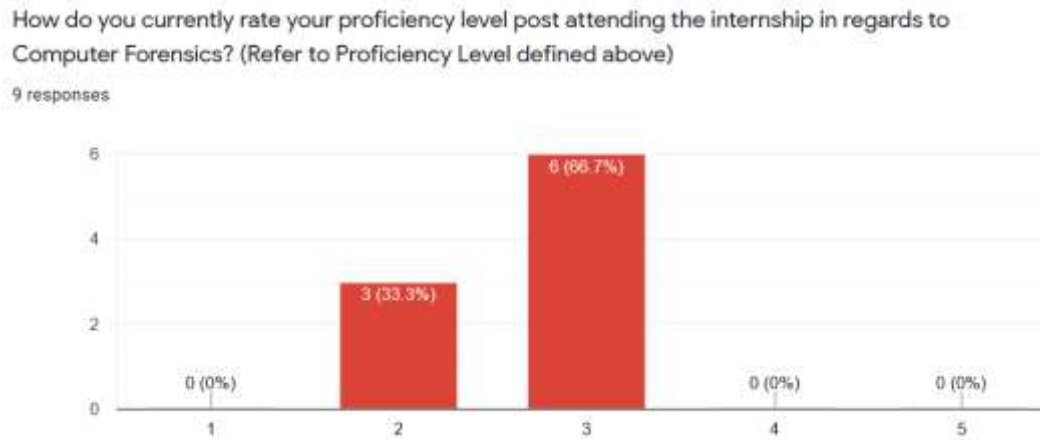


Figure 17: Participants' responses to rating their proficiency level after experiencing CR and CTF platform

4.2.6 Post Train: Development and Abilities Level

Regarding the areas of development, two-third of the participants believed that they developed the most in terms of linking theory with practice:

Having case studies along with Capture the Flag and Cyber Range, similar platforms can offer the student a complete package of understanding the different cyber security aspects, including the latest attacks and how they work. They can also practice with real-life situations to boost their technical skills and provide complete theoretical and technical knowledge. (Participant 5)

Even though many participants touched upon the positive contribution of their previous theoretical knowledge to the practical experiment, the responses of the participants also revealed that some believed the challenges they were involved in were likely to inform their theoretical understanding of relevant concepts:

Since I am in the third grade, I think I got a very good insight on cyber security in general, and when I return to my studies at the university, most of the things will be familiar to me, and I will have the knowledge already and build more knowledge on top of what I have. (Participant 3)

Another area of development mentioned by the participants was increased familiarity with forensic tools. As mentioned earlier, the participants were able to experiment with a wide variety of tools to execute various challenges. Using these tools, the participants were able to practice converting their theoretical knowledge into practical implications and better understand the extent to which they could benefit from their academic background in the field of digital forensics. The participants also concurred that their technical skills improved after using the technical gamification platform to a significant extent. For example, one participant stated that he was able to demonstrate his skills in and understanding of cyber security attacks, thanks to what he had learned in the training program. The participant also mentioned that he was able to improve his theoretical skills as he developed an “in-depth theoretical understanding of” (Participant 6) a variety of concepts on which they worked. Figure 18 depicts the participant responses to the same.

In this experiment program, the participants executed some practices that played a vital role in raising their technical skills gradually as they progressed with working on the challenges. Furthermore, the participants singled out the role of talks with business leaders as a crucial element of the training program: “In addition to the cyber range and capture the flag platforms, I would say the talks by cyber security experts were very inspiring and I learned a lot from them” (Participant 8).

2) In your honest opinion, what are the most important elements from the list above that helped up scale your technical hands on skills and expanded your horizon and understanding about Cyber Security that you would want to be included even in your academic year at university/college? Kindly elaborate.

9 responses

Battle Room 9 and Capture the Flag Platform. In addition, the expert talks and site visits, I think it would be very helpful to expose students as soon as possible.

other than the cyber range and CTF, I would say the talks by cyber security experts were very inspiring and I learned a lot from them

every single point that has been listed. From meeting industry experts and leaders to summarizing our work, I got exposed to up-to-date cyber security concerns and threats. practiced and improved my theoretical knowledge and assisted me in putting the most of my effort to learn more about cyber security on my own. Summarizing our work helped to remind me of what I have been exposed to, the things that interest me and decide the next steps to take. Universities should expose students to the market so the students can pick the right path and dedicate themselves to a field they are passionate in and additionally have a basic knowledge of all other fields within cyber security.

Regarding technical hands-on skills, I believe that access to certain platforms such as the Cyber Range and the CTF challenges were extremely helpful.
If I had access to these platforms during my first or second year of university, I believe I would have been much further along the path of developing my technical hands-on skills.

Figure 18: Participants responses to the important elements that increased the level of hands-on technical skills

Some participants pointed out that these talks were especially useful in making them more familiar with various sectors within the broader field of digital forensics as well as receiving career advice from cybersecurity leaders with proven achievement records in the field. Furthermore, Participant 1 stated that he wished he could have experienced similar events at earlier stages of his university life because he thought these events could have provided various progressive advantages when they were starting to construct a career path for themselves.

The second most commonly mentioned source of development was the extent and breadth of the mentorship they received during the program. For example, Participant 1 mentioned that the mentorship was exceptionally useful, thanks to the specific pieces of

advice they received from mentors, which were usually based on their own experiences in various situations within their careers. In a similar vein, Participant 4 stated that having an expert to guide them throughout their journey as emerging professionals was an invaluable asset that he would like to have had experienced earlier as a university student. The participants also referred to the specific features of the capture the flag and cyber range platforms to indicate that they were able to build significant technical skills that are deemed extremely helpful and useful for their future careers.

Some participants stated that visiting sites, summarizing and presenting the work they had done during the program, and the sessions on introduction to computer forensics were among the specific benefits availed from the experiment program as an effective and efficient ground for their professional development. Lastly, almost all participants mentioned a belief for significant self-development during the program, but they also indicated a self-perceived need for further improvement. To this end, 6 of the participants stated a need for further practice through similar tools:

As I do have the basic knowledge of forensics and how to use it in certain scenarios, I need more practice and development in technical skills. The internship has provided basic skills and information that will relate to most of the fields and companies. (Participant 9)

In a similar vein, Participant 4 stated that although she gained a lot of knowledge, there were still a lot of skills, knowledge and abilities she needed to learn to be able to feel confident in her skills further. Moreover, two participants pointed out that they needed more input and exposure to theoretical knowledge in digital forensics in addition to practical applications in the field. For instance, Participant 1 said, “I still feel more exposure is necessary to become truly intermediate or reach advanced/expert levels” and

argued that he is prepared to take part in training programs in the future to enhance his capabilities in this regard.

4.2.7 Post Train: Suggestions and Feedback

Lastly, the participants were also asked about their suggestions as to what additional platforms and approaches need to be introduced for undergraduates at their universities so that they could develop solid technical hands-on skills. The analysis of their responses revealed that the most prevalent suggestion concerned offering activities that focused on hands-on practice in earlier stages of students' training at universities. For example, to support this argument, Participant 7 stated that if he had had access to such training platforms during his first or second year of university, he would have made a lot more progress in terms of developing his hands-on technical skills. Similarly, Participant 5 argued that students at the university should be exposed to hands-on platforms as early as possible because the platforms they used included challenges that were quite likely to support their professional needs and skills.

Another suggestion related to mentoring in university-based programs. As mentioned earlier, the mentoring participants received during the training program was identified as one of the most valuable practices that resulted in significant amounts of self-perceived professional development on the participants' part. In a similar manner, they argued that similar mentoring opportunities should be created for learners at the university. In support of this argument, Participant 4 made the following comment: "Introducing mentoring similar to what I had would be amazing as well." The third suggestion was related to making students more familiar with the market and its players so that they could gain professional experience while learning at the university.

Moreover, one of the participants stated his belief that students could get a lot of benefits from such partnerships between academic institutions and market representations: “I also believe that universities should look into partnerships with established certification organizations to provide students with the training necessary to receive valuable certification such as OSCP and CISSP, which are offered by Offensive Security and ISC2, respectively” (Participant 7). In similar feedback, another participant argued that “universities should expose students to the market so that the students can pick the right path and dedicate themselves to a field they are passionate about and additionally have a basic knowledge of all other fields within cyber security” (Participant 6). Figure 19 depicts the participants’ responses to the same.

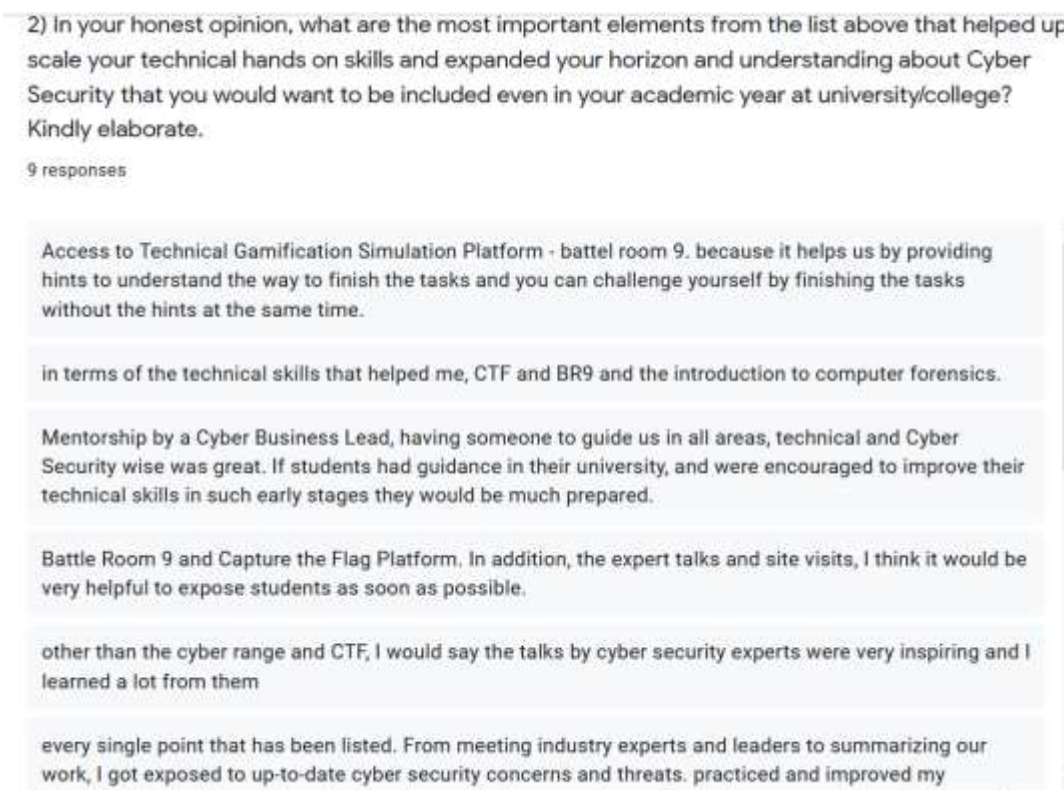


Figure 19: Participants responses to the important elements of the TGSP

The final suggestion touched upon the need for more practice at the undergraduate level. Several participants made the case that academic outcomes were prioritized over professional gains during training at the university, which prevented learners from acquiring valuable practice-based skills that were much needed in the professional practice. To overcome this barrier, two of the participants called for more activities that focus on actual hands-on practice at the university level. According to Participant 7, this challenge could efficiently be dealt with by introducing such technical gamification platform where learners could practice against simulated real-world environment that is akin to those in the real world: “I believe that online lab environments need to be implemented at universities for students to practice their hands-on technical skills, such as VHL (Virtual Hacking Labs) or HTB (Hackthebox).”

4.2.8 Post Train: Platform Preference

Finally, the last question that all the study participants were asked was, “*which of the two training platforms provided higher learning and acquiring technical skills outcomes, i.e., the cyber range or the capture the flag platform.*” Participant 1 mentioned that the CTF is more of a platform that will urge a contestant to search deeply and vertically onto a topic in order to be able to find a flag. However cyber range was more about having a structured simulated real-world scenario where the learner needs to work to solve the objectives for a given scenario. 5 out of the 9 participants shared that they found the CTF to be more fun and interesting to work on in relation to challenges because it did not have the hint function and helped them learn more about the topics through exploration and searching the Internet. However, 4 out of the 9 participants found the cyber range platform to be a more effective tool to learn and acquire hands-on technical

skills and pointed out that the hints helped them to learn and solve the scenarios eventually.

Nevertheless, all participants concurred that regardless of which platform provided significant hands-on technical skills, both of the platforms were invaluable tools that were not only to gain and acquire hands-on technical skills but provide a simulated real-world environment mimicking what may be found in the actual career life. Appendix 9 presents the use of MAXQDA in order to exhibit the results from the post train phase questionnaire.

4.3 Summary

This chapter explained in detail the results obtained from one-on-one interviews, and post-train survey questionnaire responses. The post train responses covered a variety of critical elements such as, the knowledge gained, skills developed using both cyber range and capture the flag platforms. Moreover, it covered post train responses in regards to the participants' confidence and proficiency level post hands on experience of TGSP. As well as captured suggestion and feedback from the participants on further ways that can be introduced to enrich the experience and upscale of the skills.

In the next chapter, chapter 5 lays out the design and development of the cybersecurity skills dashboard. The chapter also explains the different components of the dashboard, (i.e., the architectural diagram, the internal programming and the validation of the dashboard application).

Chapter 5: DESIGN AND DEVELOPMENT OF CYBERSECURITY SKILLS PERFORMANCE DASHBOARD

As stated by (Eckerson, 2010), a dashboard is a performance management system, that is usually used to monitor productivity. Also, according to (Few, 2013) a dashboard is a visual display of the most important information needed to achieve one or more objectives that have been consolidated on a single computer screen so it can be monitored at a glance. In this research work, the contribution the researcher made was to design and develop a Cybersecurity Skills Performance Dashboard that reflects participants' learnings of the knowledge, skills, and abilities.

The outlook of the Dashboard App is a user interface that includes visual components such as charts, graphs, and indicators of the hands-on technical skills portrayed by each participant. The dashboard app also includes an overall leaderboard that visually displays the participants with the highest scores and significant technical skills set.

The ultimate purpose of this designed and developed skills performance dashboard app is to act as a nation-wide skills performance dashboard to be able to provide a true assessment of the actual hands-on technical skills that are currently available to be benefitted from and those that need to be developed further by creating home-grown skills development initiatives and campaigns.

Furthermore, this performance dashboard app can act as an invaluable tool for businesses to be able to identify the cybersecurity professionals that they need most by searching for the technical skills that the business needs the most to fulfill an active role

they have. Also, this performance dashboard can act as a reference for the cybersecurity professional as a credible information that they can provide as evidence to various businesses about the technical skills they have acquired over time and are continuously developing.

This chapter includes description and explanation of the sections that builds the overall design and development of the cybersecurity skills performance dashboard. These sections are the design and development of the dashboard app, the architectural diagram of the dashboard, the internal programming of the dashboard, the overall interface and components of the dashboard, and the validation of the development of the dashboard.

5.1 Development of the Dashboard App

The Cybersecurity Skills Performance Dashboard (CSPD) was designed in Microsoft Excel using VBA (Visual Basic for Application) programming. The VBA programming inside an Excel spreadsheet is a dangerous source of malicious and destructive programs. For that reason, Excel has a Security Check before allowing any kind of macros in VBA. Once a user opens the Dashboard App, an alert pops up about the security verification of Excel as shown in Figure 20. The user needs to “Enable the Macros” for the dashboard application as shown in Figure 21 for it to work seamlessly; otherwise, some features of the Dashboard App will not run. However, if the security message does not pop up when opening the App, the user needs to close all Excel windows and attempt to open it again.

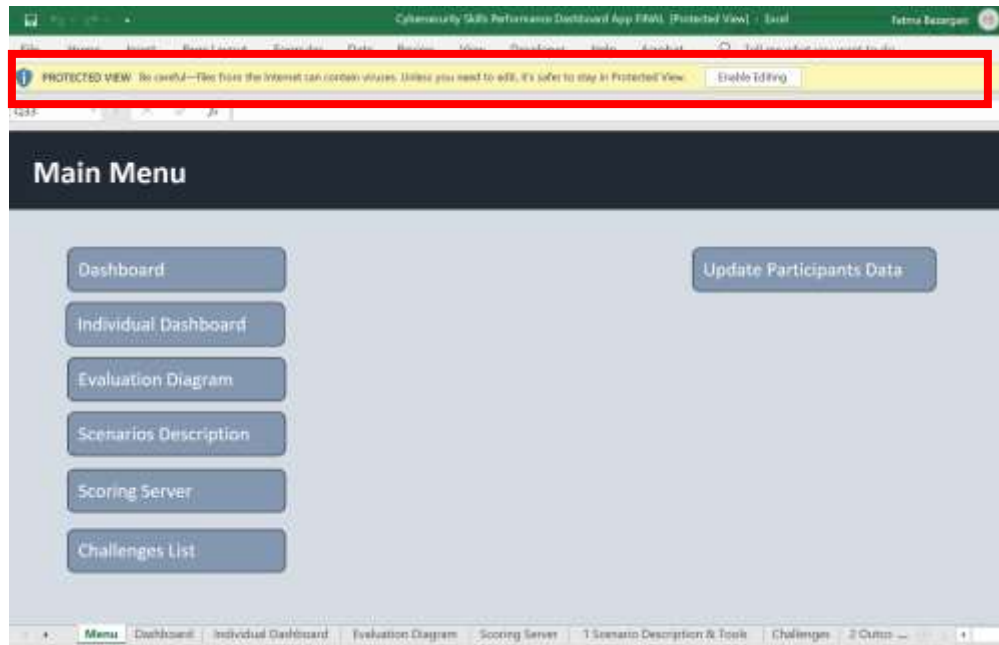


Figure 20: Cybersecurity Skills Performance Dashboard App - Main Panel



Figure 21: Enabling Macros for Dashboard App

5.2 Architectural Diagram of the Dashboard

This section shall provide a description of the cybersecurity skills performance dashboard stakeholders and the software architectural diagram of the dashboard. The C4 model was used to represent the architecture of the skills performance dashboard. The C4 model stands for context, containers, components, and code. It is a set of

hierarchical diagrams that can be used to describe the software architecture at different zoom levels (Brown, 2018).

5.2.1 Skills Performance Dashboard Stakeholders

The cybersecurity skills performance dashboard (CSPD) shall be used by many stakeholders and/or beneficiaries for several reasons. Figure 22 depicts the skills performance dashboard beneficiaries, followed by the reasons beneficiaries might find the dashboard instrumental.

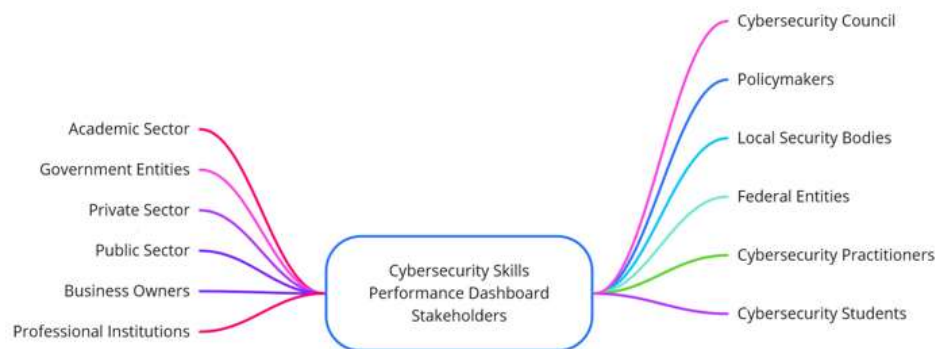


Figure 22: Cybersecurity Skills Performance Dashboard Stakeholders

As depicted in the figure above, the stakeholders can be benefitted from the skills performance dashboard as follows:

- UAE Cybersecurity Council (CSC): having a UAE nationwide cybersecurity skills performance database/repository to understand the current cybersecurity skills and talents available in the UAE and what is missing.
- UAE Policymakers: have the required visibility into the cybersecurity skill pool available and from which universities and entities to be able to better improve on

the current policies and to generate the required reports in regards to the talent and skills available.

- Local security bodies: shall have the required visibility in order to assign annual budgets to introduce capacity building campaigns to upscale the required skills and talent.
- Government/Federal/Public/Private and Business Owners: to have the required visibility to select the required cybersecurity professionals in order to meet and fulfill their cybersecurity organizational requirements as part of their cybersecurity team.
- Cybersecurity students and professionals: shall act as a platform that can record their current technical hands-on skills and act as a credible platform to provide a true assessment of their technical skills to their employers.
- Academic Sectors and Training Institutions: shall act as the entities that will enrich the dashboard database with real-time information on the training programs completed by the cybersecurity professionals. They will also be able to view the information from the dashboard to get enlightened on ways to introduce other various training programs that will fulfill the various skills required by the policy makers.

5.2.2 Architectural Diagram for CS Skills Performance Dashboard

Software architecture diagrams are meant to be used to communicate to an audience how can we go about building a certain software system and how the software system works. For the purpose of creating the architectural diagram for the cybersecurity skills performance dashboard the C4 modeling was used. C4 stands for context,

containers, components, and code. It is a set of hierarchical diagrams that can be used to describe the software architecture at different levels (Brown, 2018).

The architectural diagram for the cybersecurity performance dashboard consists of three different levels. These are:

1. **Level 1: System Context Diagram:** this is the first level of the software architecture diagram. It shows the built of the software system, the different main components that comprises the software system, other systems it connects with and the people that interact with the system. Figure 23: is the system context diagram for cybersecurity skills performance dashboard.

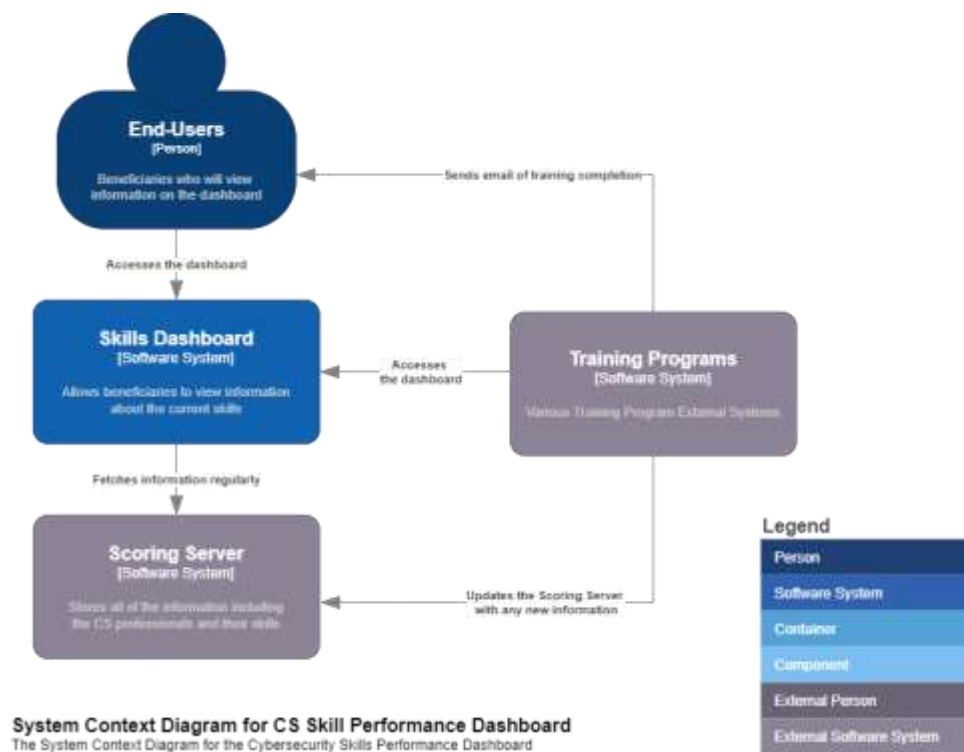


Figure 23: System Context Diagram for CS Skills Performance Dashboard

The description of the system context diagram for the CS skills performance dashboard depicted above is as follows:

- a. End-Users (Person): answers the question of who is using the system and this represents the beneficiaries as mentioned previously (i.e., cybersecurity professionals, policy makers, educational institutions, professional training institutes, local security authorities, public and private sector, etc.) these users view the dashboard and get visibility into the existent skills as portrayed by the cybersecurity professionals, the skills that needs to be further developed, and other pertinent information.
 - b. Skills Dashboard (Software System): the box in the middle represents the cybersecurity skills performance dashboard system.
 - c. Scoring Server (Software System): is basically the backend system where the actual dashboard system gets its data from to be displayed in the user interface. The scoring server stores all the information in regards to the cybersecurity professionals, the training programs they completed, the scores, and the skills obtained, etc.
 - d. Training Programs (Software System): is an external system that feeds into the scoring server. These are all the various educational and/or training institutions that have information that can be fed in the Scoring Server.
2. **Level 2: Container Diagram:** software architects need more detail to understand the backend operating model and level 2 of the architectural diagram describes just that. Thus, to zoom into the scoring server system and this will allow us to drop down to level 2 which is known as the container diagram. A container diagram shows all of the applications and data stores and how they relate and run at

runtime. Figure 24 depicts the container diagram for the skill dashboard zoomed in the scoring server system.

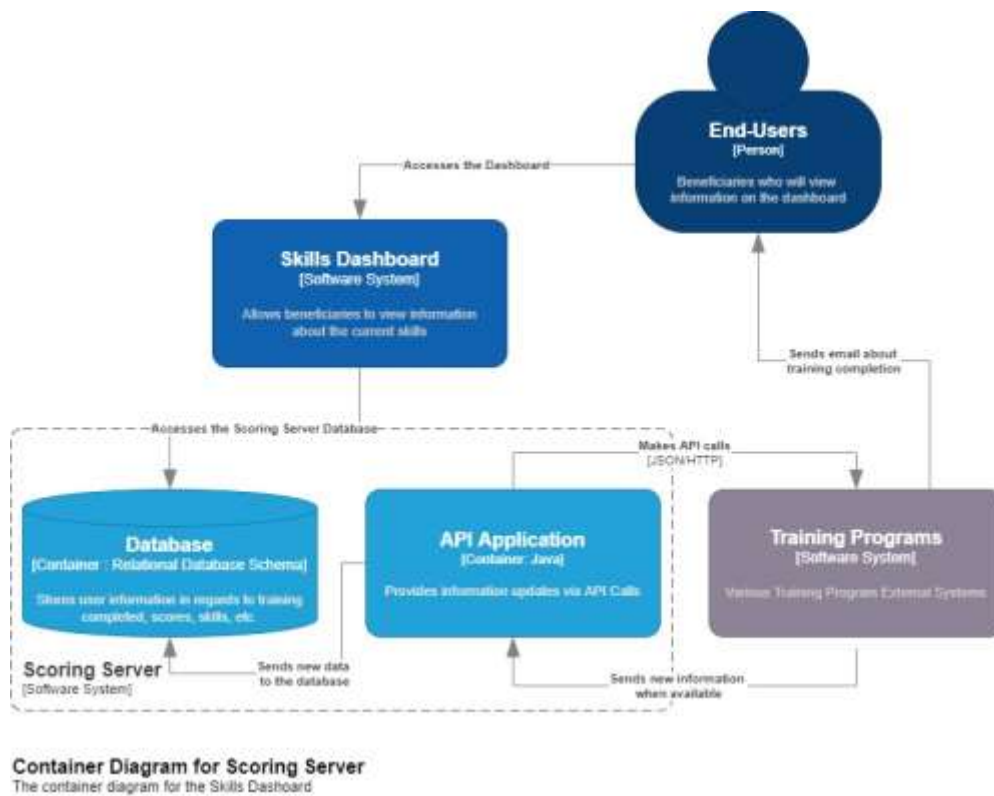


Figure 24: Container Diagram for Scoring Server

Description of Figure 24 that depicts the container diagram for the scoring server is as follows:

- a. **API Application:** is a separately deployable java container that provides the dashboard functionality via a JSON/HTTPS by making API calls to the external system of training programs to ensure that all new information in regards to the training has been fetched and consequently updates the scoring server database.
- b. **Database:** is a deployable relational database schema that stores end-user registration information, hashed authentication credentials, and access

logs. Regularly receives read and write information from the API application about any new information.

Another container diagram worth illustrating is for the skills performance dashboard itself and this is depicted in Figure 25.

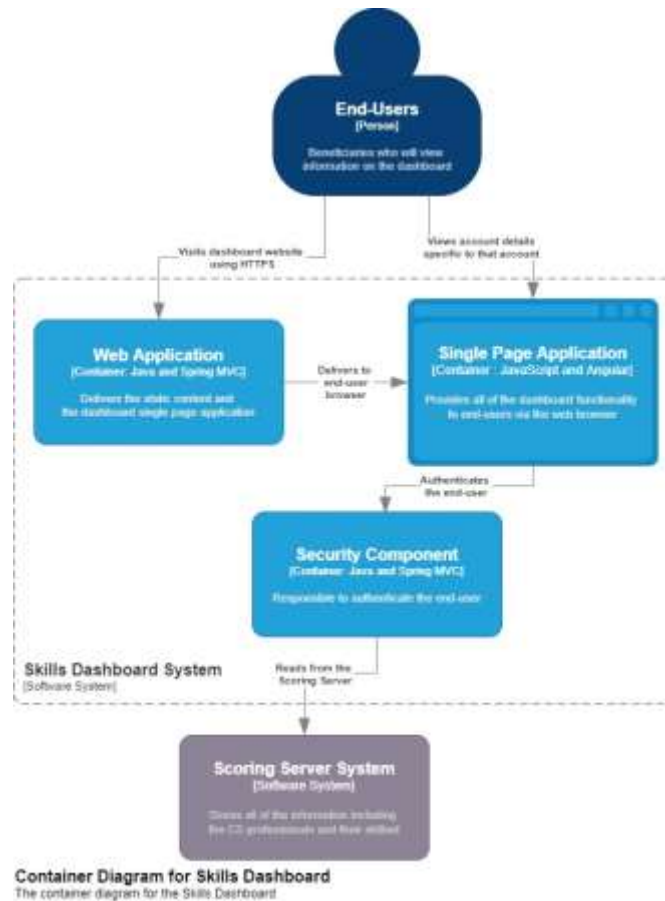


Figure 25: Container Diagram for Skills Dashboard

Description of Figure 25 that depicts the container diagram for the skills dashboard is as follows:

- a. **Web Application:** is a deployable web application container which actually is the user interface (UI) and delivers the static content of the dashboard to the end-users.

- b. **Single-Page Application:** is a JavaScript container that provides all of the dashboard functionality via a HTTPS read from the backend scoring server system.
- c. **Security Component:** is a deployable container that authenticates the end-user credentials to allow access to the information

All these containers are separately deployable systems and the lines between the containers are inter-process communication calls

- 3. **Level 3: Component Diagram:** as software architects further details are required to understand how the code base can be structured. Hence, an additional zoom in to the API application will lead to drop down to level 3 which is known as the component diagram level. Figure 26 depicts the component diagram for the skills performance dashboard system for the API application. The API application component is used mainly by the Training Programs.

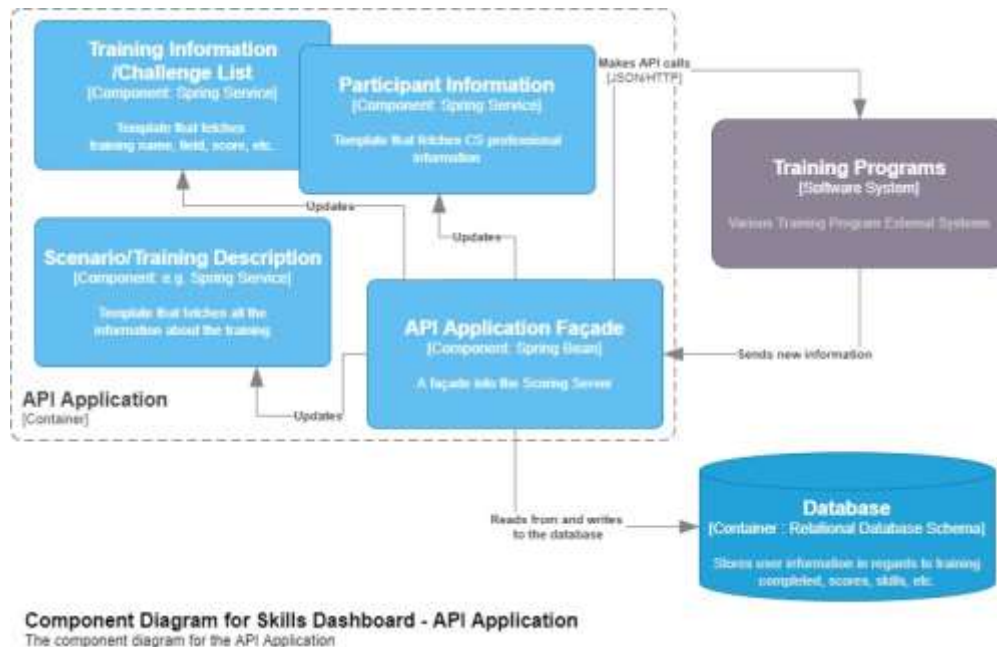


Figure 26: Component Diagram for Skills Dashboard - API Application

Below listed are the various components that sit inside the API application container.

- a. Training Information/Challenge List: is the template that needs to be updated as and when the training programs have any new training information. The template includes information that needs to be updated in terms of training name, description of it, skills gained as per the NIST/ADDA work role framework, name of the cybersecurity professional, and the score received.
- b. Participant Information: is basically the template that gets filled in and updated for a particular cybersecurity professional in terms of any new training program that has been completed and new skills added to their expertise.
- c. Scenario/Training Description: is the informational interface that gets updated with any new training program that has been added to the dashboard and was not there previously. This provides the beneficiaries with information about all the training programs that has been attended so far by the cybersecurity professionals.
- d. API Application Facade: once the Training Programs system has new updates it makes an API call to the API Application Façade to send the information updates and the Façade sends the update to the Scoring Server database.

It is to be noted that the architecture diagram is not intended to dig deeper in the code structure which is level 4 and known as the class diagram as that is not the scope of this research study.

The user interface data flow diagram for the skills performance dashboard is depicted in Figure 27.

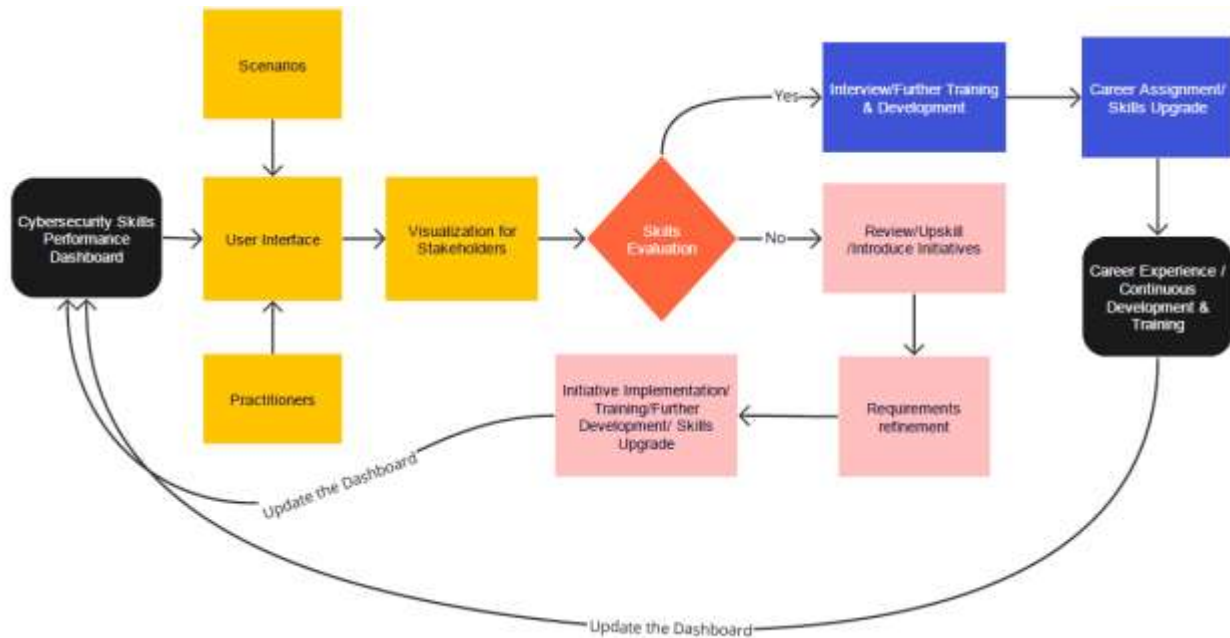


Figure 27: Architectural Operating Diagram Skills Performance Dashboard

As depicted in the figure above the dashboard operates in the following way:

1. The User Interface is available for public viewing with no requirement to enter any credentials.
2. The User Interface gets updates whenever a cybersecurity practitioner executes successfully on any given scenario.
3. The User Interface act as a visualization dashboard for all the stakeholders.
4. Stakeholders can evaluate the available skills of the practitioner through the dashboard to either:

- a. If the stakeholder is satisfied with the existing skills, they can contact the practitioner for an interview;
 - b. If the stakeholder is unsatisfied with the existing skills or foresees a skills gap proceeds to introduce the needed capacity building initiatives to shorten the skills gap. This is fulfilled by defining the requirements and introducing the needed training and development programs.
5. Once stakeholder interviews the practitioner, they provide him/her with a career opportunity and this enables the practitioner to build further experience to their technical skills through practical hands-on work experience.
6. The dashboard is considered a living repository of cybersecurity skills and talent and gets updated and maintained on regular basis.

5.2.3 CS Skills Performance Dashboard – Scenario Walkthrough

In this section, for the ease of understanding the way the dashboard work is listed as follows:

1. The end-user visits the website where the skills performance dashboard software system is placed using HTTPS.
2. The request is made to a web application which returns the static content to the end-user.
3. The end-user uses his/her login credentials using the single-page application placed on the web application.
4. Once the credentials are verified via the security component the information regarding that end-user is displayed.

5. The information stored in the scoring server database is regularly updated as and when new information is available.
6. The scoring server API application makes API calls to the external system of various entities that offer training programs based on fulfilling three templates that is:
 - a. Participant form information: this is the template in regards to all the information of the cybersecurity professional that has attended the training program and completed it.
 - b. Scenario/Training description: this is the template in regards to all the information of the training program that the cybersecurity professional has attended, title of it, description of it, period of training, and skills obtained;
 - c. Training information/challenge list: this is the template in regards to all the information of the training program that the cybersecurity professional has attended, score of the participant, skills obtained, and so on.
7. Once a cybersecurity professional attends a training course/program at a given training program institute that is connected with the dashboard system. The training program external system sends the updates based on the above 3 templates to the API application façade of the scoring server system.
8. Consequently the API application façade sends the data to the scoring server database so that the database is updated with new information as and when arrived.

5.3 Description of the Internal Programming

As discussed previously, the Skills Performance Dashboard App has automation procedures written in VBA scripting, as well as pivot tables to perform automatic calculations. In this section description of these automation features are explained.

5.3.1 Scripting in Visual Basic Editor

The scripts were written in VBA and may be accessed by the Visual Basic Editor. The user can access the Editor by the shortcut Alt+F11 or from the menu Developer/Visual Basic as shown in the Figure 28 below.

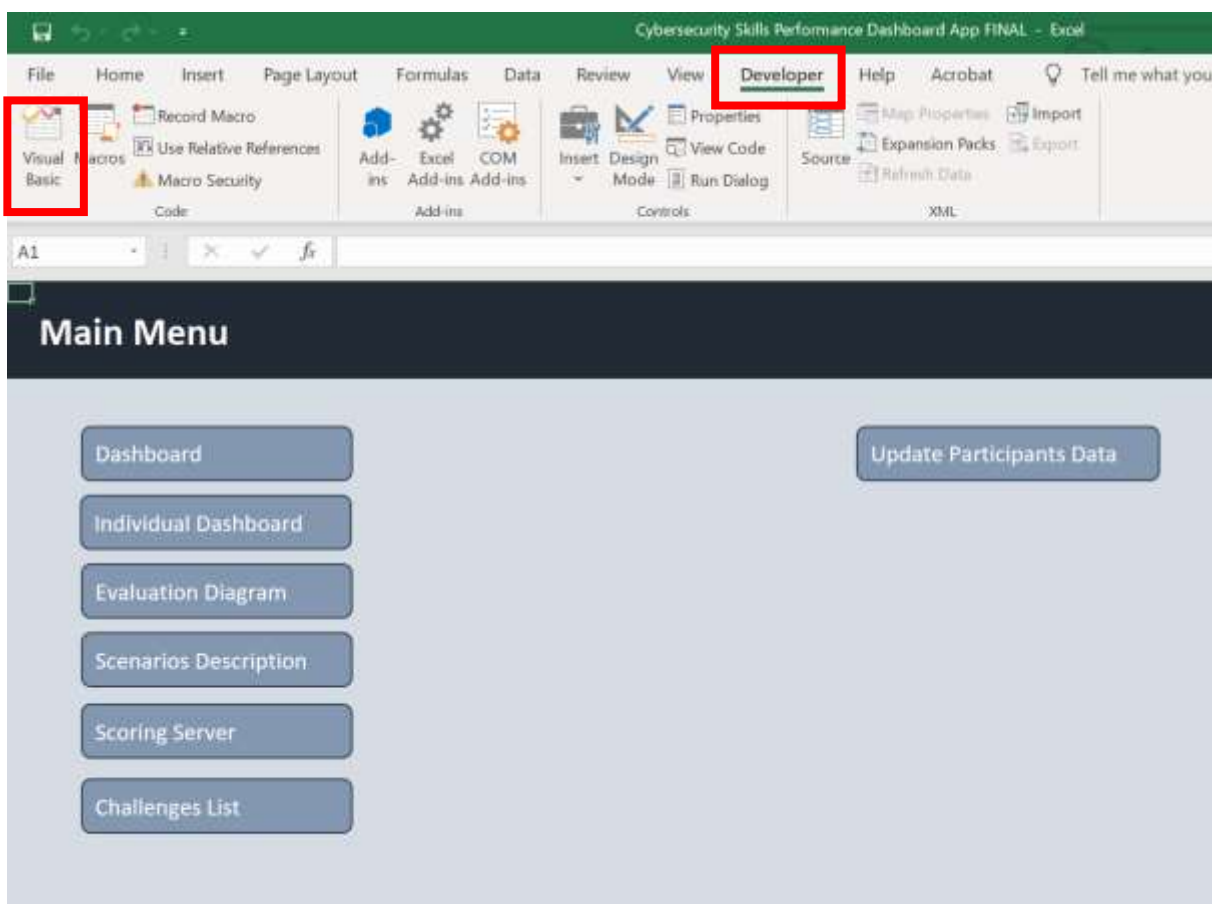


Figure 28: Dashboard App - Visual Basic Editor

The scripts developed for the Skills Performance Dashboard App are placed in Modules Folder as shown in the Figure 29 below.

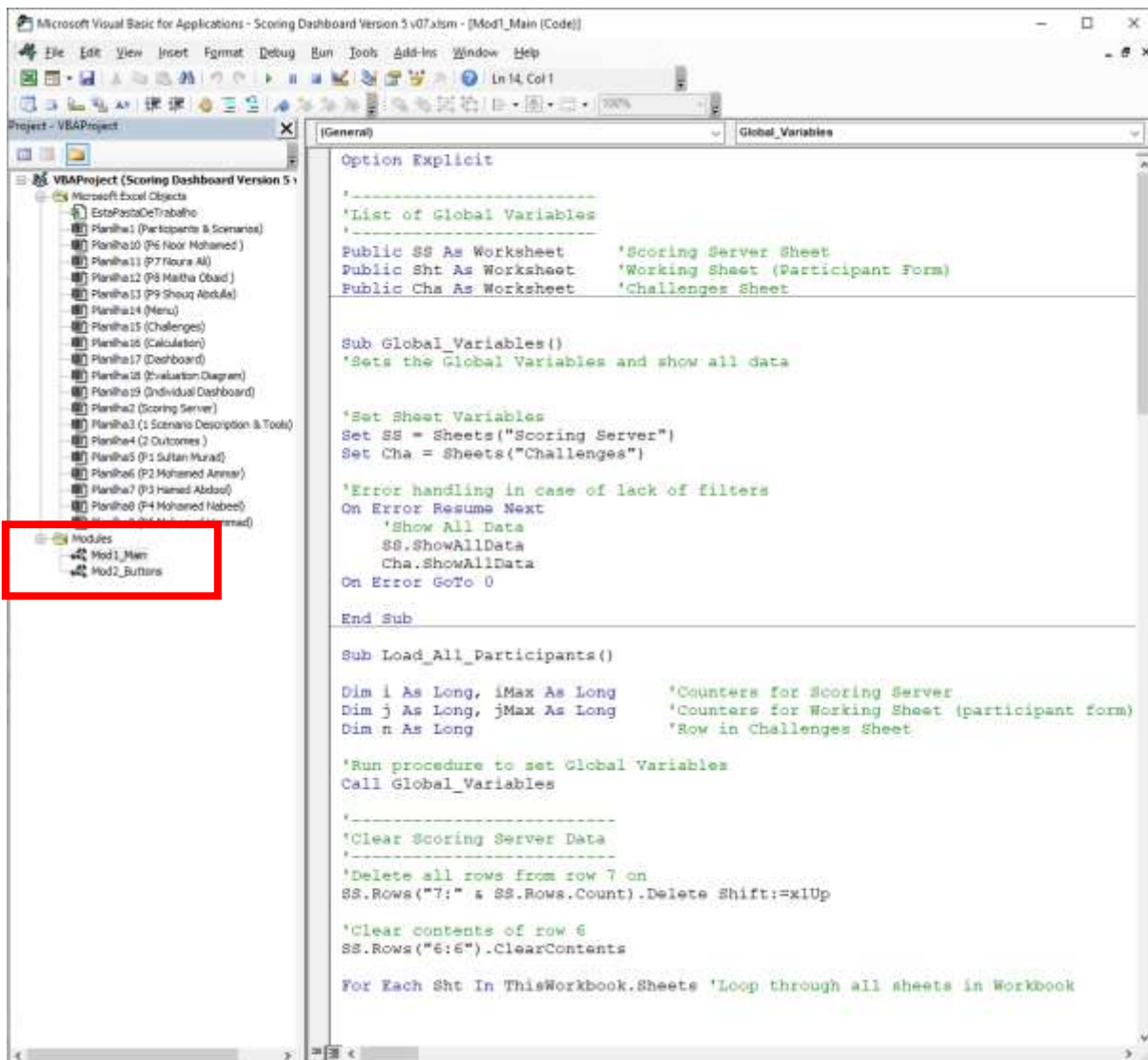


Figure 29: Dashboard App - Mod1_Main Program

In the module “Mod1_Main” is program that deals with the data transfer between the Participant Form and the Scoring Server whereas in module “Mod2_Buttons” program the simple navigation modules are saved. The commands in VBA scripts have the font color blue and black. The text in green are the comments left by the researcher to facilitate

the understanding and the future maintenance of the scripts as depicted in the Figure 30 below.

```

Option Explicit

'-----
'List of Global Variables
'-----
Public SS As Worksheet    'Scoring Server Sheet
Public Sht As Worksheet   'Working Sheet (Participant Form)
Public Cha As Worksheet   'Challenges Sheet

Sub Global_Variables()
'Sets the Global Variables and show all data

'Set Sheet Variables
Set SS = Sheets("Scoring Server")
Set Cha = Sheets("Challenges")

'Error handling in case of lack of filters
On Error Resume Next
    'Show All Data
    SS.ShowAllData
    Cha.ShowAllData
On Error GoTo 0

End Sub

Sub Load_All_Participants()

Dim i As Long, iMax As Long    'Counters for Scoring Server
Dim j As Long, jMax As Long    'Counters for Working Sheet (participant form)
Dim n As Long                  'Row in Challenges Sheet

'Run procedure to set Global Variables
Call Global_Variables

'-----
'Clear Scoring Server Data
'-----
'Delete all rows from row 7 on
SS.Rows("7:" & SS.Rows.Count).Delete Shift:=xlUp

'Clear contents of row 6
SS.Rows("6:6").ClearContents

For Each Sht In ThisWorkbook.Sheets 'Loop through all sheets in Workbook

```

Commands

Comments

Figure 30: Dashboard App - Commands and Comments

In the next sections description of each program is elaborated on.

5.3.2 List of Global Variables

The List of Global Variables consists of the name of the sheets that will be used by the VBA procedures as shown in Figure 31.

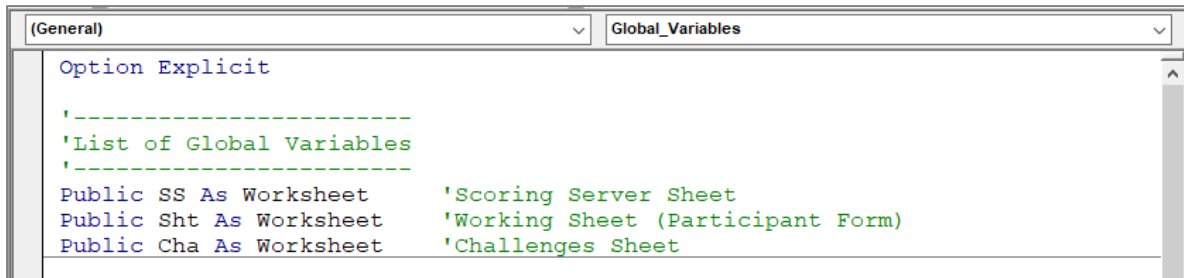


Figure 31: List of Global Variables

Procedure “Global_Variables”

The procedure “Global_Variables” as shown in Figure 32 sets the name of the sheets for the global variables described in previous section.

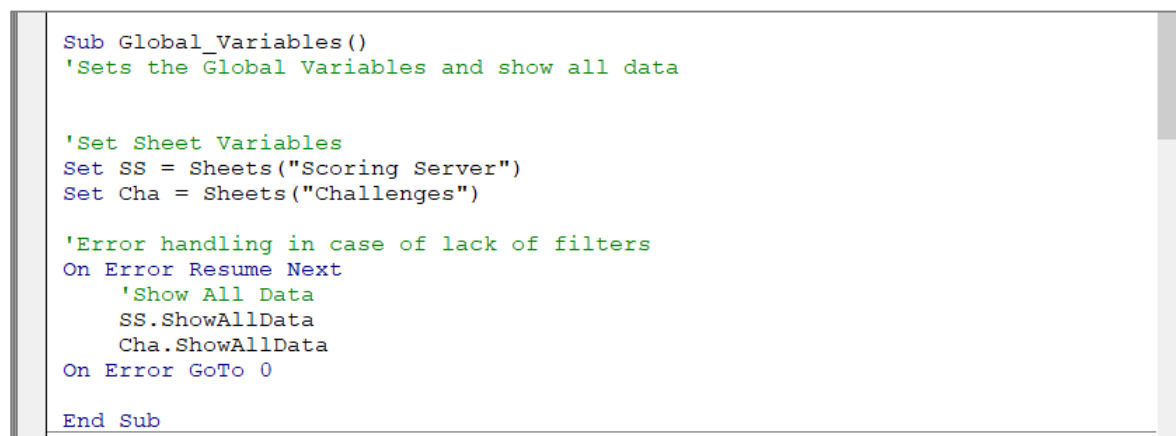


Figure 32: Procedure "Global_Variables"

Procedure “Load_All_Participants”

The procedure “Load_All_Participants” as shown in Figure 33 is responsible for transferring the data from all the Participant Forms to the Scoring Server.

```

Sub Load_All_Participants()

Dim i As Long, iMax As Long      'Counters for Scoring Server
Dim j As Long, jMax As Long      'Counters for Working Sheet (participant form)
Dim n As Long                    'Row in Challenges Sheet

'Run procedure to set Global Variables
Call Global_Variables

'-----
'Clear Scoring Server Data
'-----
'Delete all rows from row 7 on
SS.Rows("7:" & SS.Rows.Count).Delete Shift:=xlUp

'Clear contents of row 6
SS.Rows("6:6").ClearContents

For Each Sht In ThisWorkbook.Sheets 'Loop through all sheets in Workbook

    'Check if the Sheet is a Participant Form
    If Sht.Range("A1") = "Participant Form" Then

        'Error handling in case of lack of filters
        On Error Resume Next
        'If there is a filter, show all data
        Sht.ShowAllData
        On Error GoTo 0

        'Take Last Row of Participant Form
        jMax = Sht.Range("A" & Sht.Rows.Count).End(xlUp).Row

        'Take Last Row of Scoring Server
        iMax = SS.Range("A" & SS.Rows.Count).End(xlUp).Row

        'Adjust iMax if the Table is Empty
        If iMax = 6 And Len(SS.Range("A6")) = 0 Then iMax = 5

        'Set Row in Scoring Server
        i = iMax
        For j = 6 To jMax 'Loop through each challenge in Participant Form

            'Add one row to the Scoring Server
            i = i + 1

```

Figure 33: Procedure “Load_All_Participants”

The main steps of this procedure are:

- Clear all previous data in Scoring Server sheet;
- Loop all the sheets, looking for ones with the title “Participant Form”;
- Read all the data in Participant Form and copy to the Scoring Server;

- In Scoring Server, fill in the additional fields “Completion”, “Skill” and “Time Spent Playing”, converting the time into decimal hours; and
- Refresh all pivot tables in the spreadsheet.

Function “Find_Scenario”

The function “Find_Scenario” as shown in Figure 34 is used by the procedure “Load_All_Participants”. The function looks for a specific scenario in Challenged Sheet and returns which row in the table this scenario is stored. If the Scenario is not found, the function returns zero.

```
Function Find_Scenario(Scenario As String) As Long
'Returns the row of the specific Scenario in Challenges Sheet

Dim i As Long, iMax As Long      'Counters for Challenges Sheet

'Run procedure to set Global Variables
Call Global_Variables

'Take Last Row of Challenges Sheet
iMax = Cha.Range("B" & Cha.Rows.Count).End(xlUp).Row

'Set Not Found value to zero
Find_Scenario = 0

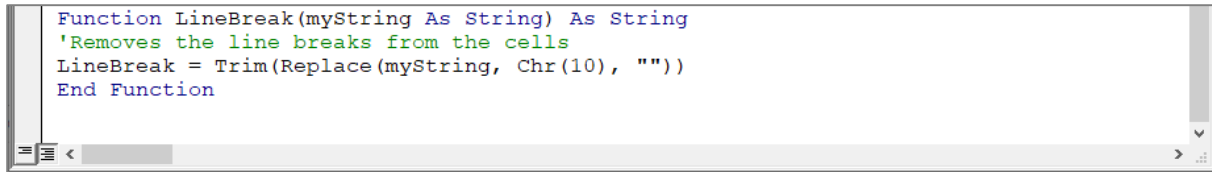
For i = 6 To iMax
    If Cha.Range("B" & i) = Scenario Then
        Find_Scenario = i
        Exit Function
    End If
Next i

End Function
```

Figure 34: Function “Find_Scenario”

Function “LineBreak”

The function “LineBreak” as shown in Figure 35 removes line breaks from the Participant Forms before the data is stored in the Scoring Sever.

A screenshot of a VBA code editor window. The code defines a function named 'LineBreak' that takes a string 'myString' as input and returns a string. The function's purpose is to remove line breaks from the input string. The code is as follows:

```
Function LineBreak(myString As String) As String
'Removes the line breaks from the cells
LineBreak = Trim(Replace(myString, Chr(10), ""))
End Function
```

The editor has a standard interface with a menu bar on the left and a scrollbar on the right.

Figure 35: Function “LineBreak”

5.3.3 Navigation Procedures

The navigation procedures, with names starting with “GoTo_” are associated to the navigation buttons in the Main Menu as shown in Figure 36. They perform only three simple steps:

- Refresh all pivot tables in the spreadsheet;
- Select the desired sheet; and
- Select the first cell (A1) in order to align the sheet view

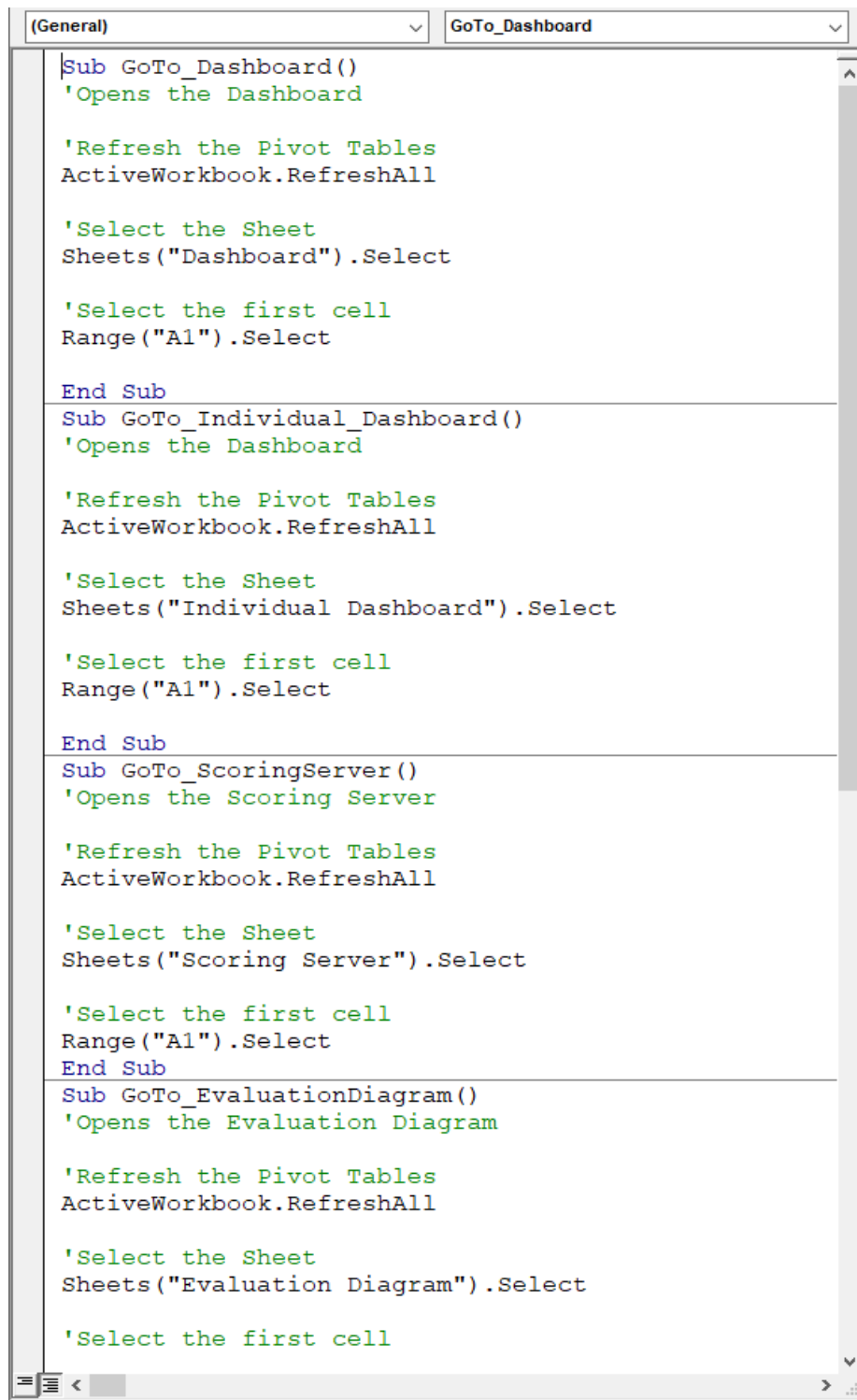


Figure 36: Navigation Procedures

5.3.4 Pivot Tables

Most of the calculations performed by the Scoring Dashboard are done by pivot tables as shown in Figure 37. The pivot tables are placed in the Calculation sheet as shown in the figure below.

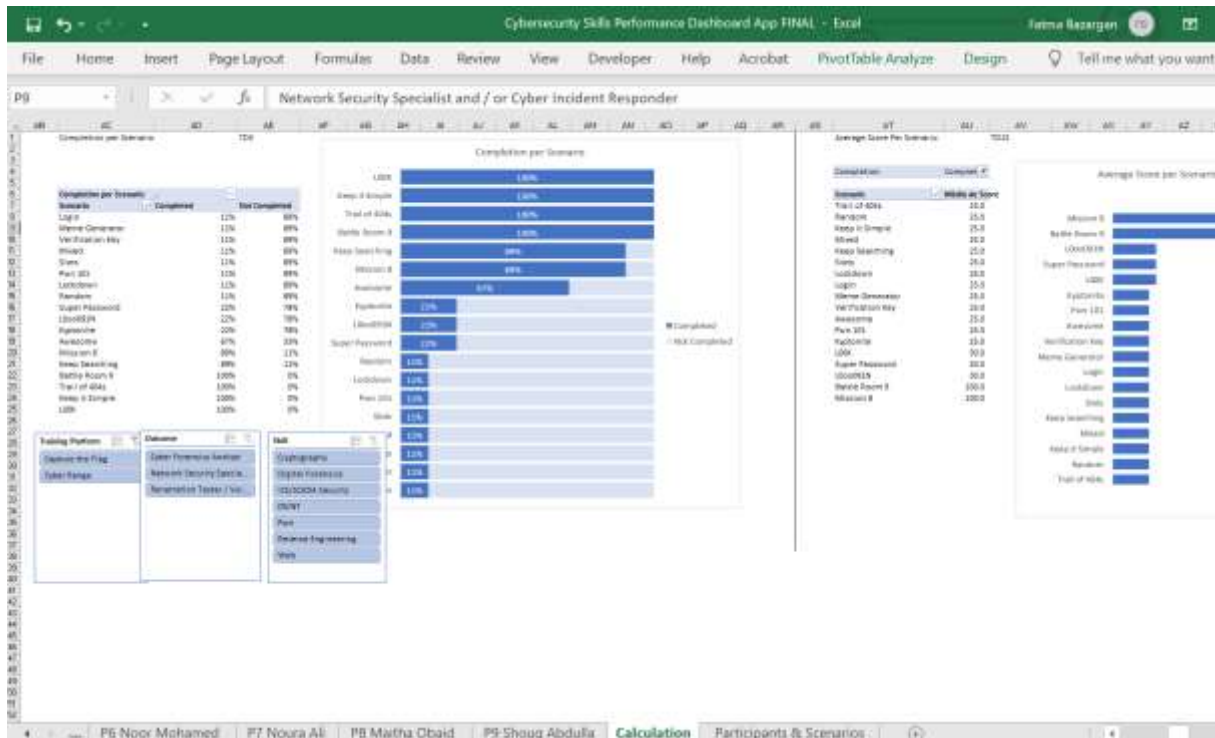


Figure 37: Pivot Tables

All the pivot tables are based on the same data source – the Scoring Server sheet. Every time the procedure updates the Scoring Server table, it also updates all the pivot table values. The charts in the dashboard are built directly from the pivot tables – they are called “pivot charts”. The pivot charts have the advantage of being updated automatically when the pivot table is updated. That is why the Dashboards are updated instantaneously when new data is inputted.

The filters in the dashboards are performed by pivot table “Slicers” as shown in Figure 38. The slicers are list of values that when selected filters the data of the pivot table dynamically.

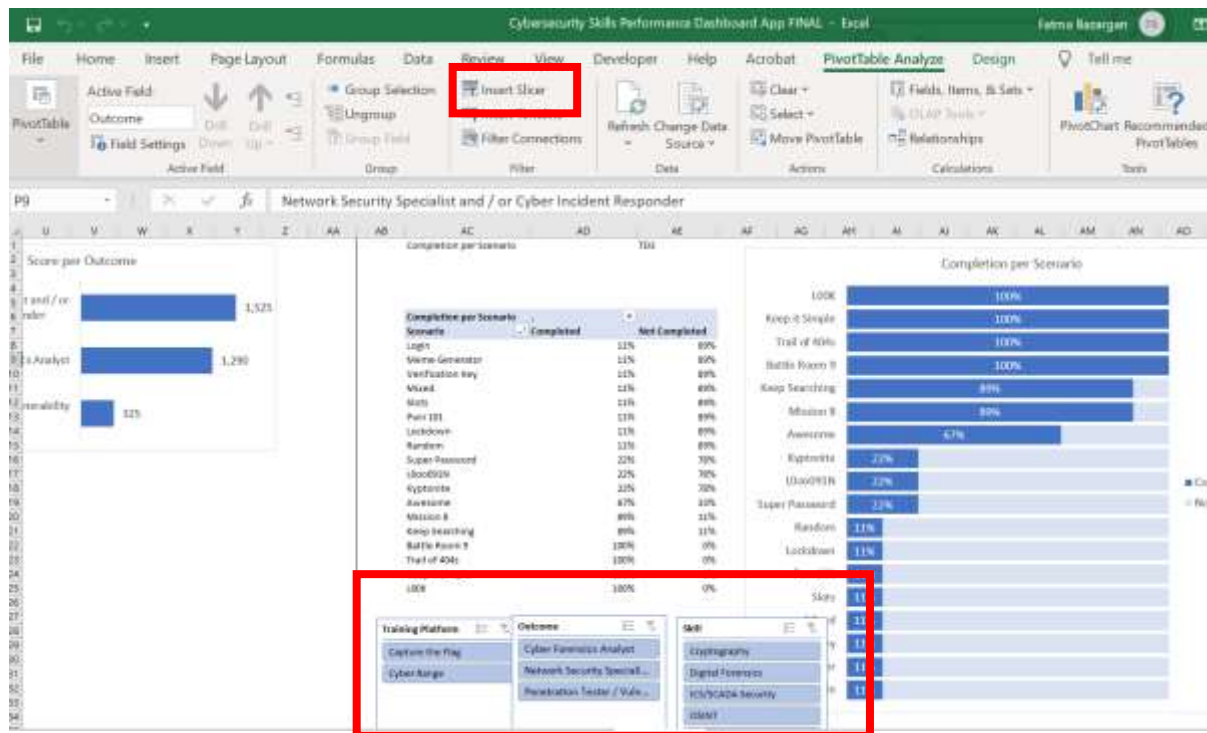


Figure 38: Filters – Slicers

5.4 Components of the Dashboard App

The Skills Performance Dashboard App has several components. This is to enable the user to organize and visualize the data in many ways. Following sections describe on each of the components in detail.

5.4.1 Main Dashboard Feature

The Main Menu can be found on the tab “Menu” of the App and includes all the various features that the Dashboard App can provide to the user as shown in Figure 39.

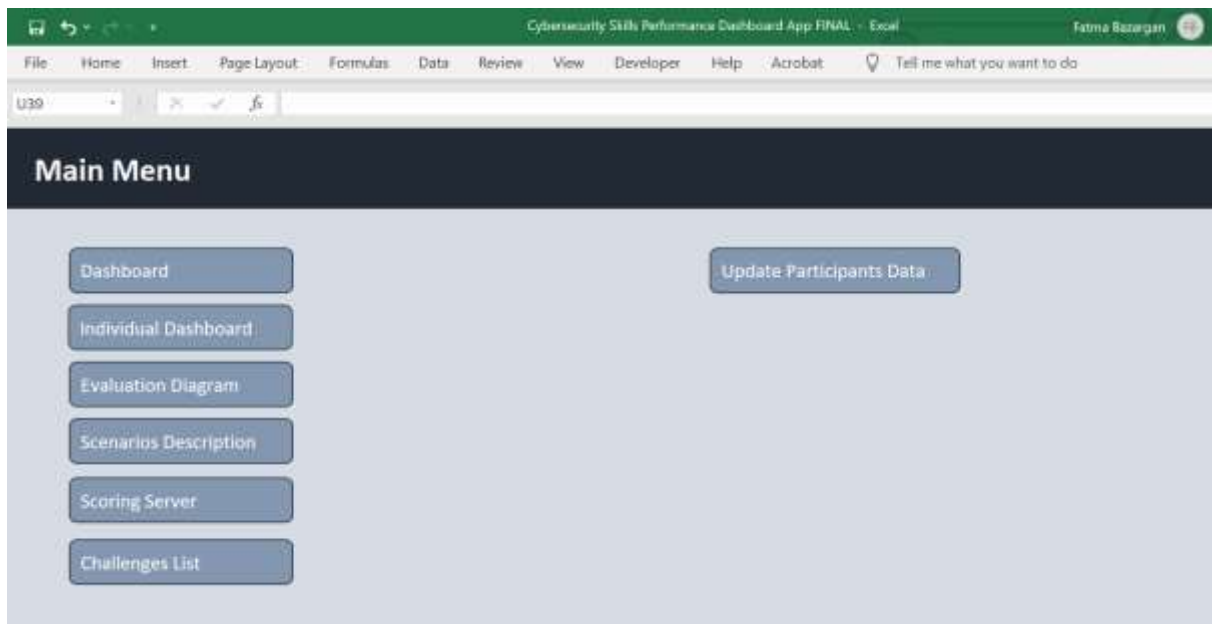


Figure 39: Main Menu - Dashboard App

Once the user opens the Dashboard App, the first step that needs to be taken for the App to work effectively is to “Update Participants Data” as shown in Figure 40. Unlike the other buttons in the Main Menu, the button “Update Participants Data” does not open any data visualization screen. Instead, it runs an internal procedure to copy/update the data from all the Participants Forms to the Scoring Server.

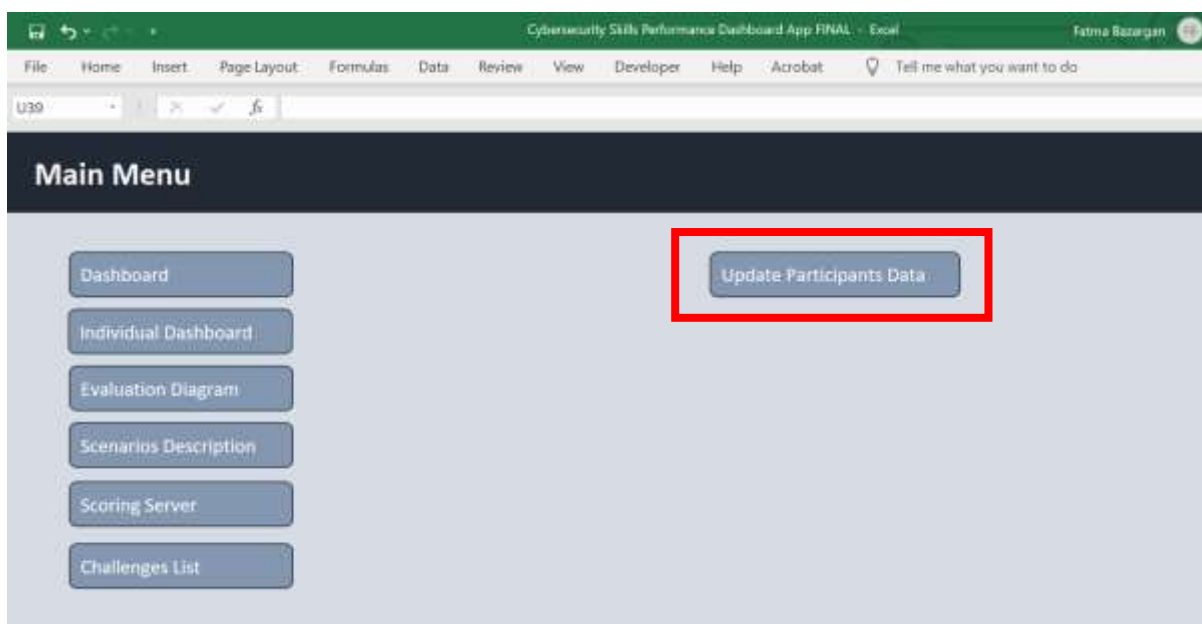
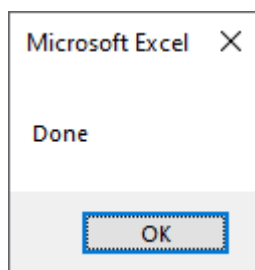


Figure 40: Dashboard App - Update Participant Data

The update process takes a few seconds. When the update process is completed, the notification below will pop up and the user may continue to navigate through the Skills Performance Dashboard App.



The user can access the general statistics Dashboard by clicking the button “Dashboard” in the Main Menu as shown in Figure 41. The upcoming sections will elaborate further on the visualization features available in the Dashboard view.

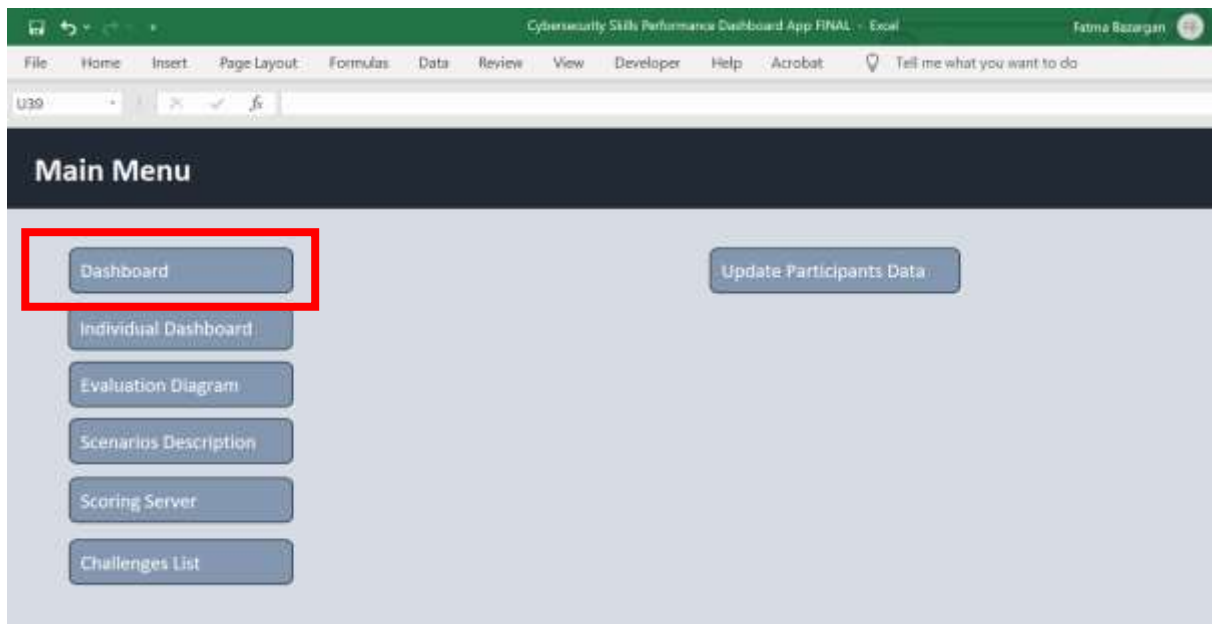


Figure 41: Dashboard App - Dashboard View

On the top panel of the Dashboard, the user may find three filter slicers to enable the user to interact with the data visualization and look for the information he/she desires as shown in Figure 42.

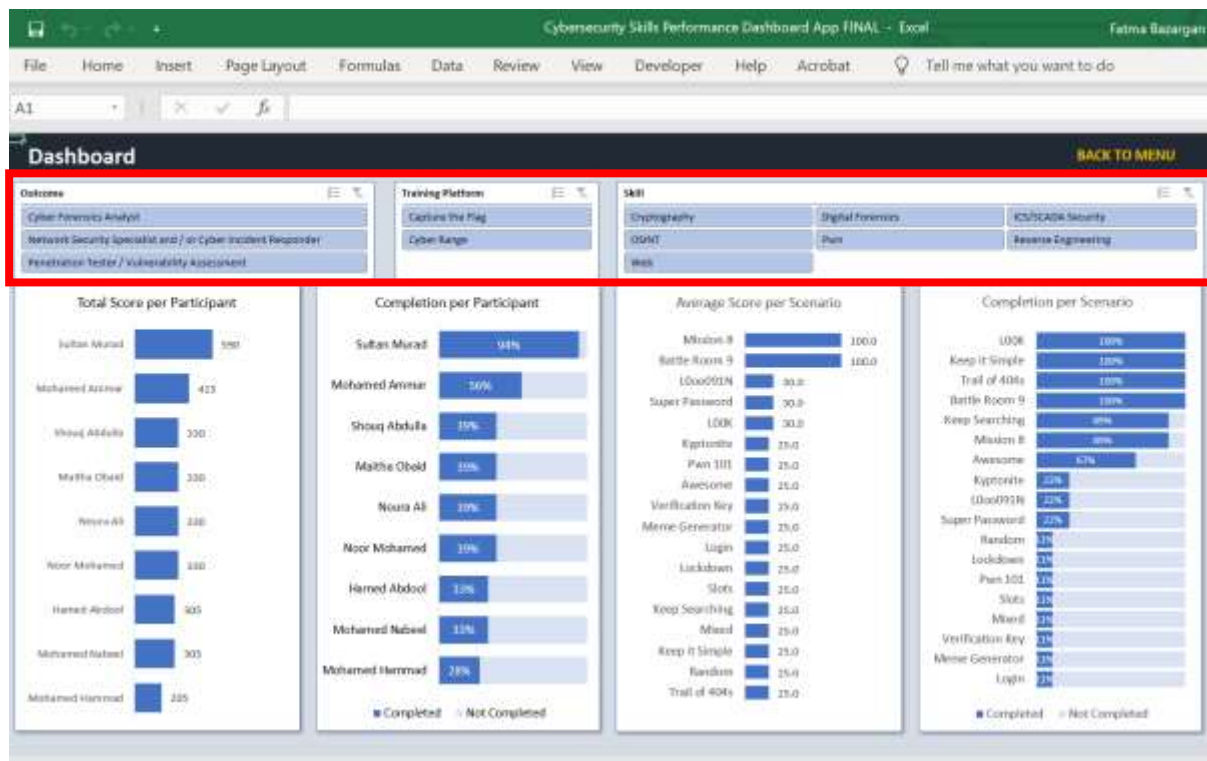


Figure 42: Dashboard App - Dashboard Visualization Statistics

In the top panel of the Dashboard view there exists three different filters that a user may apply. By clicking the buttons of “Outcome”, “Training Platform” and “Skill”, the Dashboard will update the charts and show the statistics related to the filtered features.

To navigate back to Main Menu, the user may click “Back to Menu” button in the upper-right corner of the Dashboard as depicted in Figure 43.



Figure 43: Dashboard App - Back to Menu Button

5.4.2 Individual Dashboard Feature

The Individual Dashboard has the data visualization view of each Participant in the study whose data has been on boarded to the Dashboard App. It can be accessed by clicking the button “Individual Dashboard” in the Main Menu as shown in Figure 44 below.

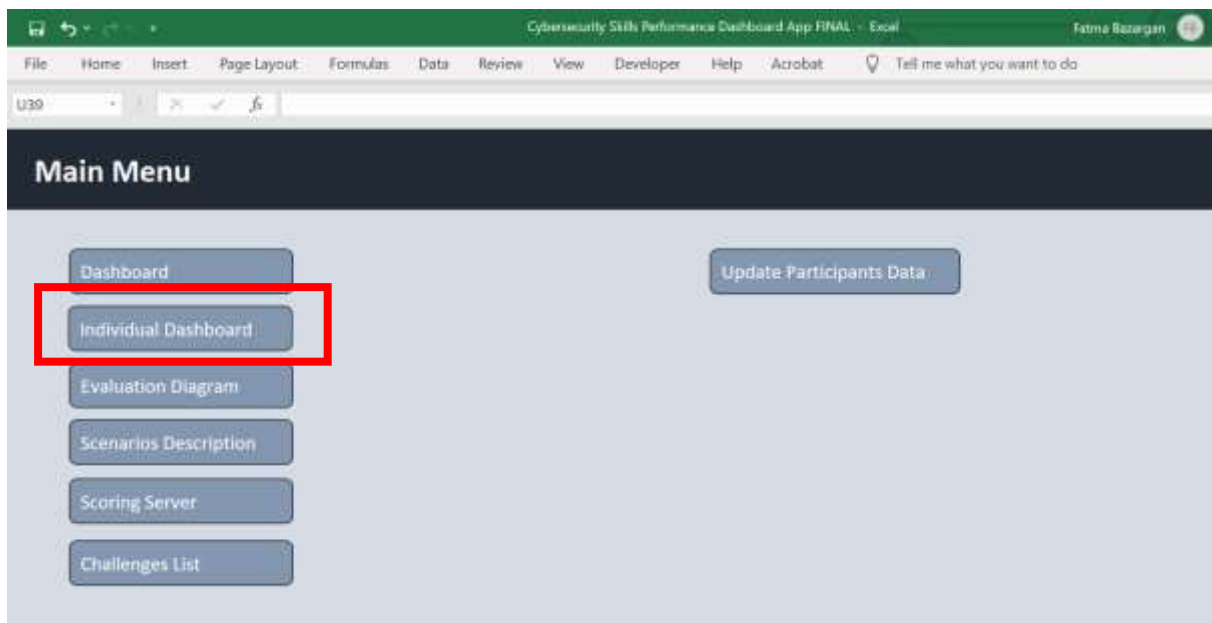


Figure 44: Dashboard App - Individual Dashboard View

If the user chooses one participant from the Participant slicer, the Individual Dashboard will show the specific data of the chosen person. On the other hand, by disabling the filters, the Individual Dashboard will show the overall data as shown in Figure 45.

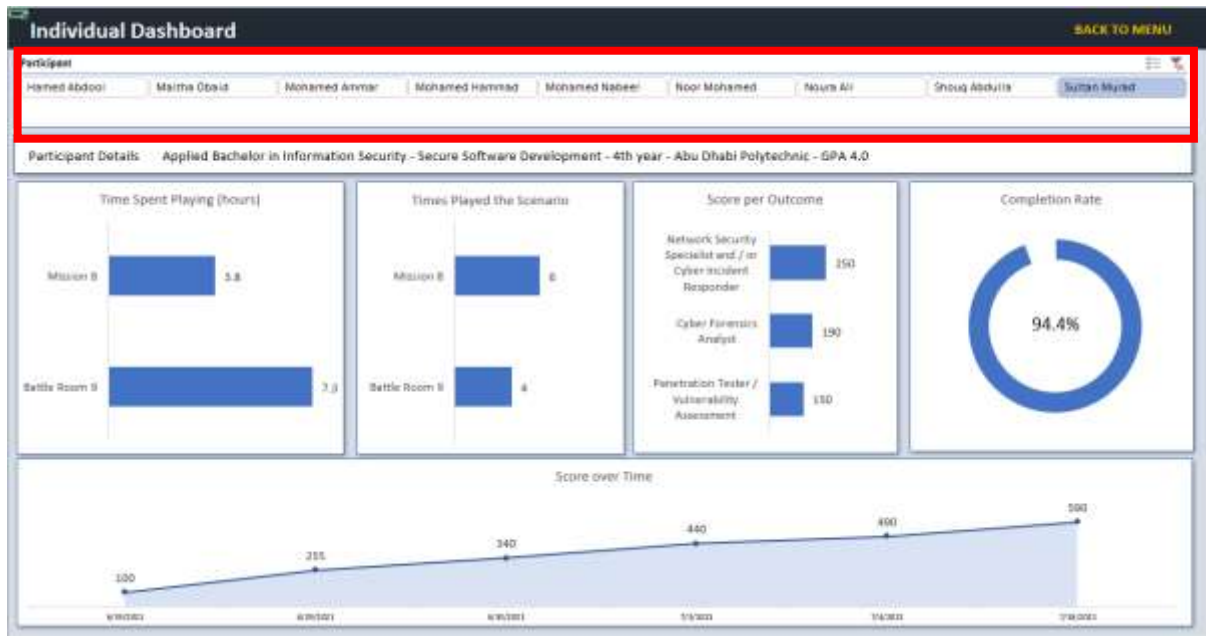


Figure 45: Dashboard App - Individual Dashboard View - Loaded

5.4.3 Evaluation Diagram Feature

The Evaluation Diagram is a visual format to show how the different Training Platforms, Scenarios, Skill Categories and Outcomes are related to one another. User can access the diagram by clicking the “Evaluation Diagram” button in Main Menu as shown in Figure 46 below.

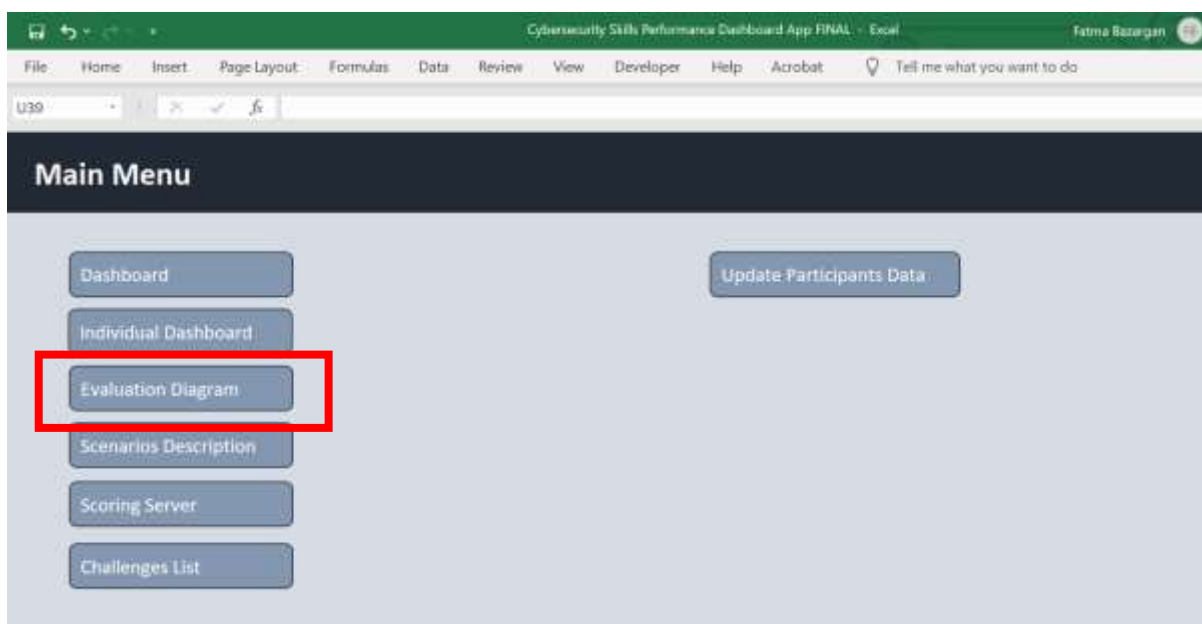


Figure 46: Dashboard App - Evaluation Diagram

The color coding in the Evaluation Diagram represents the different hands-on technical skills as shown in Figure 47. The user can visualize which hands-on technical skill is tested in each of the various Training Platforms and Scenarios by checking the circled colors, as well which skills are represented in each Outcome based on and mapped to the Abu Dhabi Digital Authority Work Role Assessment Tool as mentioned previously.

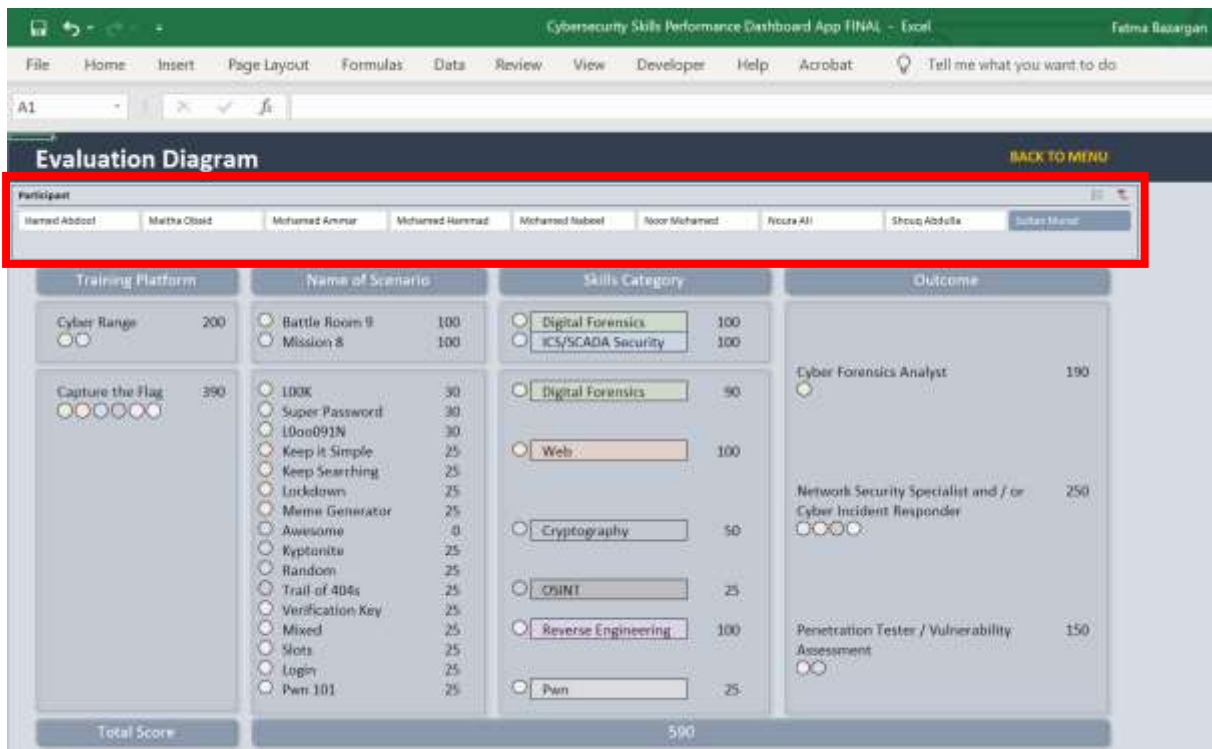


Figure 47: Dashboard App - Evaluation Diagram - Loaded

5.4.4 Scenario Description Feature

The same as in the Individual Dashboard, the user can choose one or more participants from the Participant slicer, and the score views will be updated automatically. By clicking the “Scenarios Description” in the Main Menu panel, the user can access a detailed description about each Scenario and the tools used to execute the scenario as shown in both Figures 48 and 49.

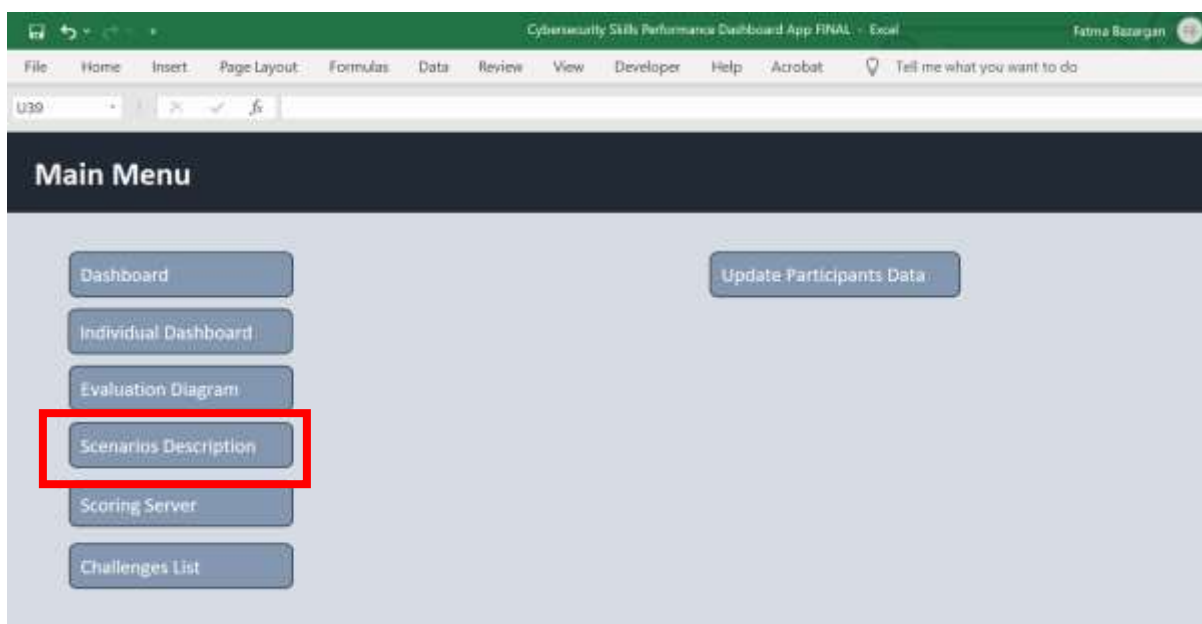


Figure 48: Dashboard App - Scenario Description

Scenario Description & Tools			BACK TO MENU
Scenario	Description of the Scenario	Tools Used	
Battle Room 9: Digital Forensics	Battle Room 9 is about a Digital Forensics different challenge comprises of 10 challenges the skills the learner develops are looking in unexpected locations / files, understanding where certain information can be found, inspecting the web, navigating Windows NTFS file system, analyzing files metadata, navigating Windows registry structure and understanding Windows executable artifacts - Ability to find date/time/type, deleted items, crack passwords, find root files, dig into history and emails.	Tools used while executing on Battle Room 9 which is a digital forensics challenge was mainly the use of Kali Linux, online decoding tools, web inspection, wayback, registry explorer, ophcrack, USB Isolation, Deode and Autopsy - using autopsy for analyzing forensics images, using ophcrack and rainbow tables to crack recovered hashes from the SAM database.	
Mission 8: Operation Ocean View	Mission 8 is about an ICS/SCADA system that has been compromised. The SCADA system has been showing 10 times higher level of objective, and an attacker has accessed the SCADA system from inside. The learner should respond to the incident that has occurred in a water treatment plant with the main goal of restoring the version of the plant to normal operations. The 4 key tasks are: verify network monitoring tools are functioning, identify the adversary IP address, block the adversary activity from entering the network, and verify that control system processes are stable and back to normal.	Tools used while executing on completing Mission 8 four objectives were use of Kali Linux: 1. Squall to complete objective 1, 2. Security Onion and Squall to complete objective 2, 3. Sslstrip and Fimrafail CVD to complete objective 3, and 4. SSH and NMAP to complete objective 4.	
Capture the Flag: Web	Various web challenges	Better utilization of Burp suite, use of python to create scripts to speed up specific tasks, understanding CSPs, content security policies, and bypassing them to pull off XSS attacks in order to get an access as an admin on a website.	
Capture the Flag: Reverse Engineering	Various reverse engineering challenges	Use of disassemblers (Binary Ninja) and Debuggers (Ollydbg and gdb) for static and dynamic analysis.	
Capture the Flag: Digital Forensics	Various digital forensics challenges	Use of Binwalk and Foremost for embedded file extraction, use of FTK imager to parse add, logical images, identify hidden information within registries with Registry Explorer and crack hashes with Hashcat and John the Ripper.	
Capture the Flag: OSINT	Various OSINT challenges	Ability to analyze dead packets and findings suspicious information, Ability to search the internet and the use of Wayback machine archive to solve the challenge.	
Capture the Flag: Cryptography	Various cryptography challenges	Ability to decrypt emoji-based encrypted messages and developing python scripts to reverse hash functions.	

Figure 49: Dashboard App - Scenario Description - Loaded

5.4.5 Scoring Server Feature

The Scoring Server is the main engine of the internal information database where the Scoring Dashboard App keeps the participants data to perform the different data visualization views described. The user can access it by clicking on the “Scoring Sever” button in the Main Menu as shown in Figure 50.

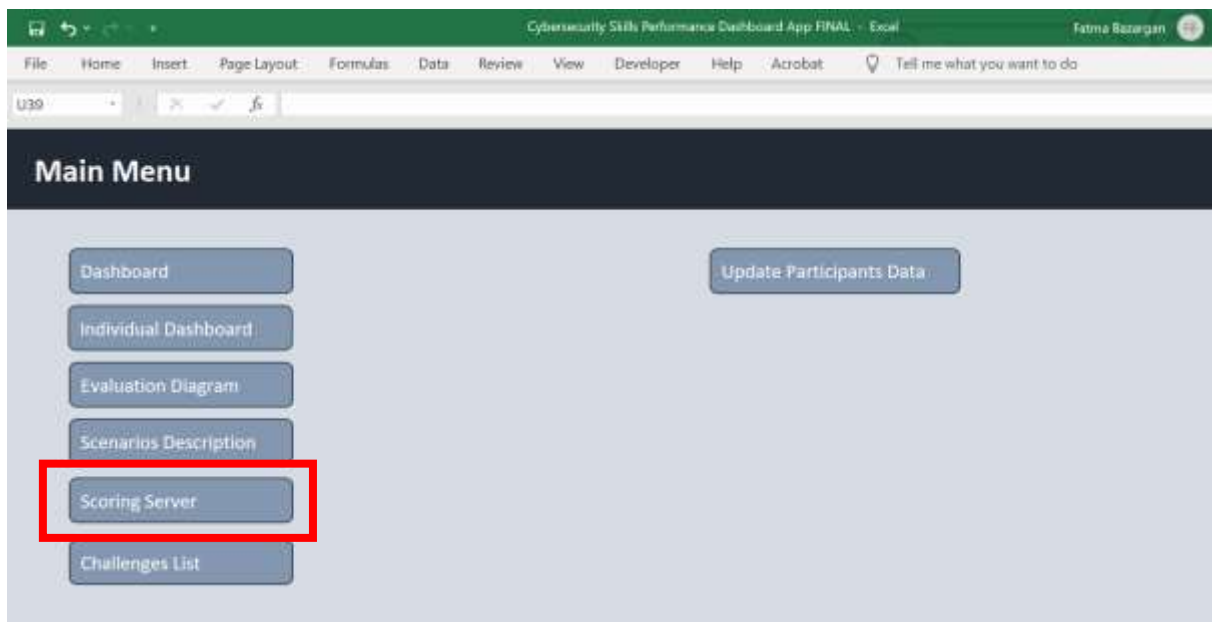


Figure 50: Dashboard App - Scoring Server

The Scoring Server table is updated and maintained by the administrator of the Dashboard App as shown in Figure 51.

Cybersecurity Skills Performance Dashboard App FINAL - Excel										Fatma Batargan	
File	Home	Insert	Page Layout	Formulas	Data	Review	View	Developer	Help	Acrobat	Tell me what you want to do
A1											
Scoring Server										BACK TO MENU	
Participant Name	Participant Details				Cell Number	Training Platform	Skills Category	Name of Scenario	Score		
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 4.8	3	Cyber Range	Digital Forensics	Battle Room 8	330	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	3	Cyber Range	ICS/SCADA Security	Mission 8	330	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	3	Capture the Flag	Digital Forensics 1	LORE	30	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	4	Capture the Flag	Digital Forensics 2	Super Password	30	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	5	Capture the Flag	Digital Forensics 3	DeadOSIN	30	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	6	Capture the Flag	WebGL	Keep it Simple	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 4.8	7	Capture the Flag	WebGL	Keep Searching	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	8	Capture the Flag	WebGL	Lockdown	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	9	Capture the Flag	WebGL	Memo Generator	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 4.8	10	Capture the Flag	Cryptography 1	Anonymous	0	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	12	Capture the Flag	Cryptography 2	Kryptonic	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	13	Capture the Flag	Cryptography 3	Randoms	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 4.8	15	Capture the Flag	OSINT	Trail of 200s	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	14	Capture the Flag	Reverse Engineering 1	Verification Key	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	15	Capture the Flag	Reverse Engineering 2	Mixed	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 4.8	16	Capture the Flag	Reverse Engineering 3	Stats	25	
Sultan Mansur	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 4.8	17	Capture the Flag	Reverse Engineering 4	Login	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.888	3	Cyber Range	Digital Forensics	Battle Room 8	330	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	3	Cyber Range	ICS/SCADA Security	Mission 8	300	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	3	Capture the Flag	Digital Forensics 1	LORE	30	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	4	Capture the Flag	Digital Forensics 2	Super Password	30	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	5	Capture the Flag	Digital Forensics 3	DeadOSIN	30	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	6	Capture the Flag	WebGL	Keep it Simple	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.888	7	Capture the Flag	WebGL	Keep Searching	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	8	Capture the Flag	WebGL	Lockdown	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	9	Capture the Flag	WebGL	Memo Generator	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.888	10	Capture the Flag	Cryptography 1	Anonymous	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	12	Capture the Flag	Cryptography 2	Kryptonic	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	13	Capture the Flag	Cryptography 3	Randoms	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.888	15	Capture the Flag	OSINT	Trail of 200s	25	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	14	Capture the Flag	Reverse Engineering 1	Verification Key	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	15	Capture the Flag	Reverse Engineering 2	Mixed	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.888	16	Capture the Flag	Reverse Engineering 3	Stats	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.508	17	Capture the Flag	Reverse Engineering 4	Login	0	
Mohamed Ammar	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.888	18	Capture the Flag	Pen	Pen 101	0	
Hamed Abdoel	Applied Bachelor in Information Security	Secure Software Development	30th year	Abu Dhabi Polytechnic	GPA 3.8	3	Cyber Range	Digital Forensics	Battle Room 8	330	
Hamed Abdoel	Applied Bachelor in Information Security	Secure Software Development	4th year	Abu Dhabi Polytechnic	GPA 3.8	3	Cyber Range	ICS/SCADA Security	Mission 8	330	

Figure 51: Dashboard App - Scoring Server - Loaded

5.4.6 Challenges List Feature

The Challenges List is the internal place where the Scoring Dashboard App keeps the available Scenarios and sets the relation between the Scenarios, Training Platforms, Skills and Outcomes as shown in as shown in Figure 52 and 53 below.

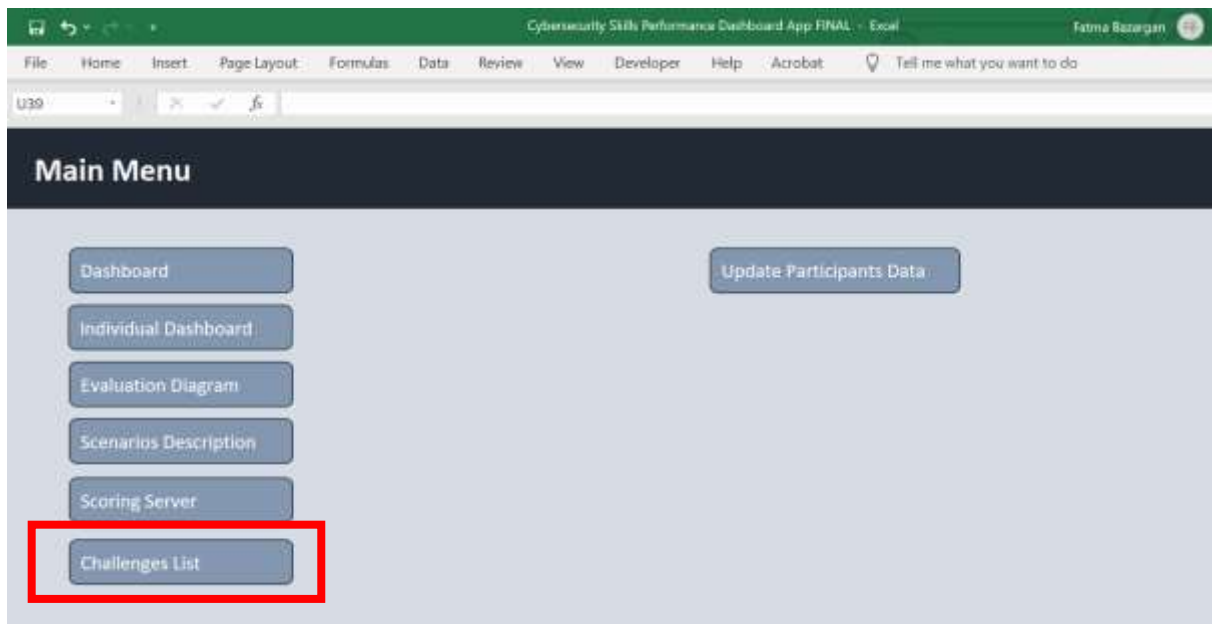


Figure 52: Dashboard App - Challenges List

The screenshot shows the 'Challenges' table in the 'Cybersecurity Skills Performance Dashboard App FINAL'. The table has five columns: Training Platform, Name of Scenario, Skills Category, Skill, and Outcome. The table contains 20 rows of data, including challenges like 'Capture the Flag', 'Cyber Range', and 'Meme Generator'.

Training Platform	Name of Scenario	Skills Category	Skill	Outcome
Capture the Flag	Awesome	Cryptography 1	Cryptography	Penetration Tester / Vulnerability Assessment
Capture the Flag	Kyptonite	Cryptography 2	Cryptography	Penetration Tester / Vulnerability Assessment
Capture the Flag	Random	Cryptography 3	Cryptography	Penetration Tester / Vulnerability Assessment
Cyber Range	Battle Room 9	Digital Forensics	Digital Forensics	Cyber Forensics Analyst
Capture the Flag	L00K	Digital Forensics 1	Digital Forensics	Cyber Forensics Analyst
Capture the Flag	Super Password	Digital Forensics 2	Digital Forensics	Cyber Forensics Analyst
Capture the Flag	L00o091N	Digital Forensics 3	Digital Forensics	Cyber Forensics Analyst
Cyber Range	Mission 8	ICS/SCADA Security	ICS/SCADA Security	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Trail of 404s	OSINT	OSINT	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Pwn 101	Pwn	Pwn	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Verification Key	Reverse Engineering 1	Reverse Engineering	Penetration Tester / Vulnerability Assessment
Capture the Flag	Mixed	Reverse Engineering 2	Reverse Engineering	Penetration Tester / Vulnerability Assessment
Capture the Flag	Slots	Reverse Engineering 3	Reverse Engineering	Penetration Tester / Vulnerability Assessment
Capture the Flag	Login	Reverse Engineering 4	Reverse Engineering	Penetration Tester / Vulnerability Assessment
Capture the Flag	Keep it Simple	Web1	Web	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Keep Searching	Web2	Web	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Lockdown	Web3	Web	Network Security Specialist and / or Cyber Incident Responder
Capture the Flag	Meme Generator	Web4	Web	Network Security Specialist and / or Cyber Incident Responder

Figure 53: Dashboard App - Challenges List - Loaded

5.4.7 Participant Form Feature

The participant form is where the administrator on board and / or updates an existing participant, as well as the Scenarios, Scores and other data concerning the participant as shown in Figure 54 below.

Cybersecurity Skills Performance Dashboard App FINAL - Excel

FileHomeInsertPage LayoutFormulasDataReviewViewDeveloperHelpAcrobatTell me

A24

Participant Form

Participant Name	Sultan Mured		Participant Details	Applied Bachelor in Information Security - Secure Software Development - 4th year - Abu Dhabi Polytechnic - GPA 4.0						
------------------	--------------	--	---------------------	---	--	--	--	--	--	--

Cell Number	Training Platform	Skills Category	Name of Scenario	Score	Completion Timestamp	Outcomes	Times Played the Scenario	Time Spent Playing		
								Hours	Minutes	Seconds
1	Cyber Range	Digital Forensics	Battle Room 9	100	19-Jun	Cyber Forensics Analyst	4	7	18	25
2	Cyber Range	ICS/SCADA Security	Mission 8	100	18-Jul	Network Security Specialist and / or Cyber Incident Responder	6	3	48	11
3	Capture the Flag	Digital Forensics 1	LOOK	30	19-Jun	Cyber Forensics Analyst				
4	Capture the Flag	Digital Forensics 2	Super Password	50	30-Jun	Cyber Forensics Analyst				
5	Capture the Flag	Digital Forensics 3	1000091N	30	30-Jun	Cyber Forensics Analyst				
6	Capture the Flag	Web1	Keep it Simple	25	19-Jun	Network Security Specialist and / or Cyber Incident Responder				
7	Capture the Flag	Web2	Keep Searching	25	19-Jun	Network Security Specialist and / or Cyber Incident Responder				
8	Capture the Flag	Web3	Lockdown	25	19-Jun	Network Security Specialist and / or Cyber Incident Responder				
9	Capture the Flag	Web4	None Generator	25	19-Jun	Network Security Specialist and / or Cyber Incident Responder				
10	Capture the Flag	Cryptography 1	Awezone	0		Penetration Tester / Vulnerability Assessment				
11	Capture the Flag	Cryptography 2	Exploitize	25	30-Jun	Penetration Tester / Vulnerability Assessment				
12	Capture the Flag	Cryptography 3	Exploitize	25	30-Jun	Penetration Tester /				

Figure 54: Dashboard App - Participant Form

The Dashboard App is being developed to be scalable and flexible in regards to onboarding any new participant to the App or update on the existing participant. In addition, the administrator of the App can add as many scenarios, outcomes, and skills as required. All the administrator needs to do is to duplicate one the Participant Form

from the system and fill in the data of the new participant. After the new data has been entered, the user needs to click on the “Update Participants Data” in the Main Menu to update the data into the system and the data visualization to work correctly.

5.5 Validation of the Cybersecurity Skills Performance Dashboard

This section of the chapter validates the effectiveness and efficiency of the cybersecurity skills performance dashboard. This is conducted through displaying the dashboard results for each of the 9 participants as explained in the following subsections.

Appendix 5 presents the exported raw data results from the Cyber Range and Capture the Flag platforms for the participants. These raw results were fed into the backend dashboard repository and through the programming mentioned previously were display for each of the participant interface.

5.5.1 Participant 1 Skills Performance Evaluation

Participant 1, is a male 4th-year student who majored in Applied Bachelor in Information Security (specialization of Secure Software Development) with excellent academic status, secured 4.0 GPA and is studying at Abu Dhabi Polytechnic Institute. The participant scored the highest amongst all other participants in the study as he was able to complete 17 scenarios. He scored a completion rate of 94.4%. He was able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, reverse engineering, web security, pwn, and OSINT. His playing time in battle room 9 was 7hours and mission 8 3hours. The number of times participant 1 played battle room 9 was 4 times and mission 8 was 6 times. Figure 55 depicts the

Participant 1 Cybersecurity Skills Performance level. The participant secured 250 points in network security specialist/cyber incident responder related tasks, 190 points in cyber forensics analyst related tasks, and 150 points in penetration tester/vulnerability assessment related tasks.

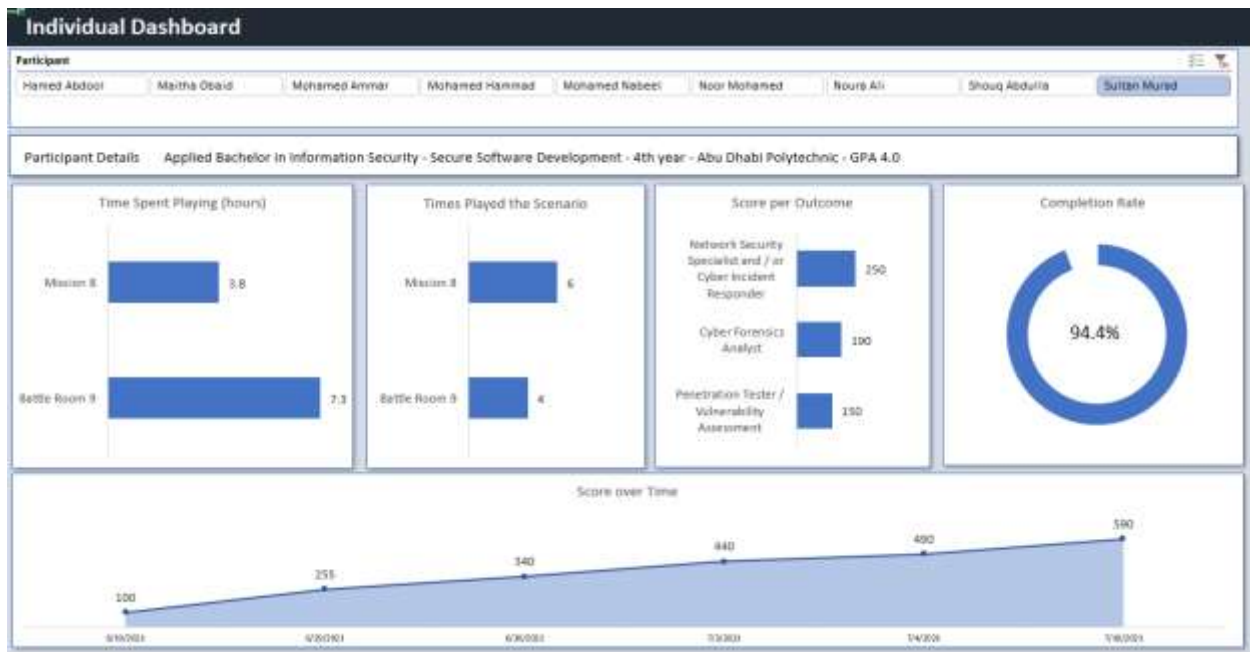


Figure 55: Participant 1 Cybersecurity Skills Performance Level

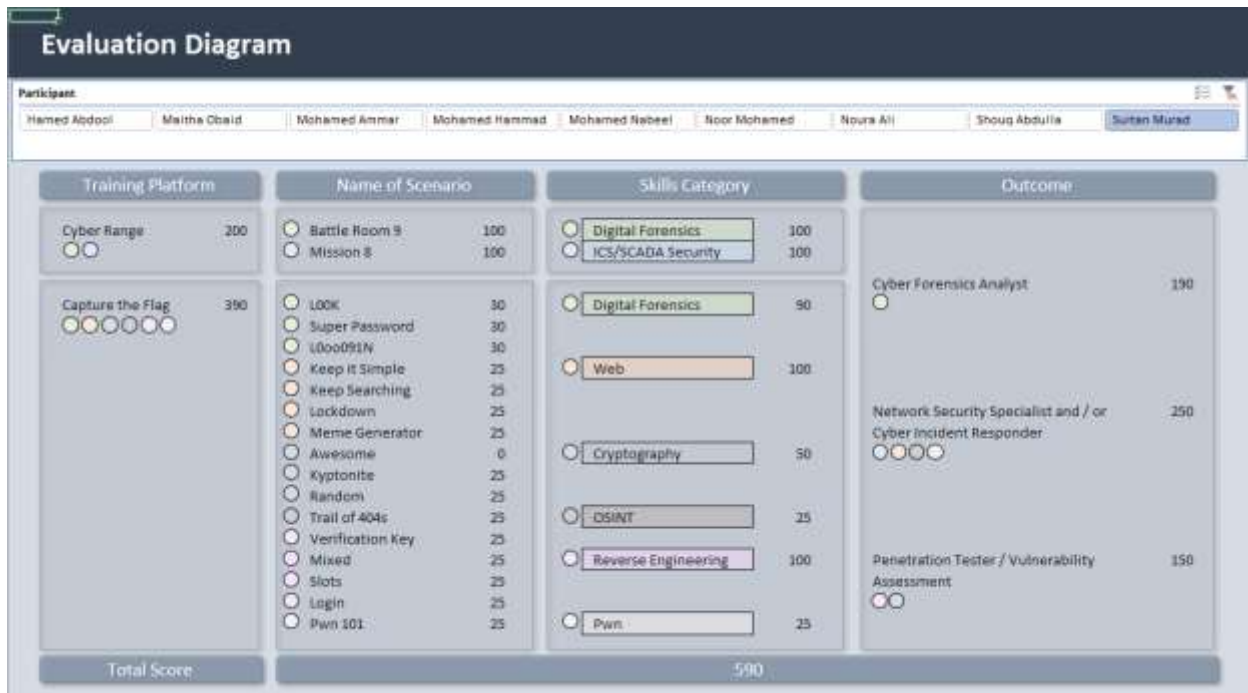


Figure 56: Participant 1 Training Platform Scores and Outcomes

Figure 56 depicts the training platform scores and outcomes for participant 1. As earlier shown, the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, he secured 390 points for capture the flag (CTF) challenges. This concluded that the participant acquired a significant set of hands-on technical skills executing these various 17 challenges on both platforms. Based on the technical skills acquired, it indicates that the participant possesses technical skills that qualify him to fill in technical roles such as cyber forensics analyst, network security specialist / Cyber incident responder, and penetration tester/vulnerability assessment.

5.5.2 Participant 2 Skills Performance Evaluation

Participant 2, is a male 4th-year student who majored in Applied Bachelor in Information Security (specialization of Secure Software Development) with excellent

academic status, secured 3.986 GPA and is studying at Abu Dhabi Polytechnic Institute. The participant scored the second highest amongst all other participants in the study as he was able to complete 10 scenarios. He scored a completion rate of 55.6%. He was able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, web security, and OSINT. His playing time in battle room 9 was 15hours and mission 8 1hour. The number of times participant 2 played battle room 9 was 6 times and mission 8 was 11 times. Figure 57 depicts the Participant 2 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist/cyber incident responder related tasks, 190 points in cyber forensics analyst related tasks, and 50 points in penetration tester/vulnerability assessment related tasks.



Figure 57: Participant 2 Cybersecurity Skills Performance Level

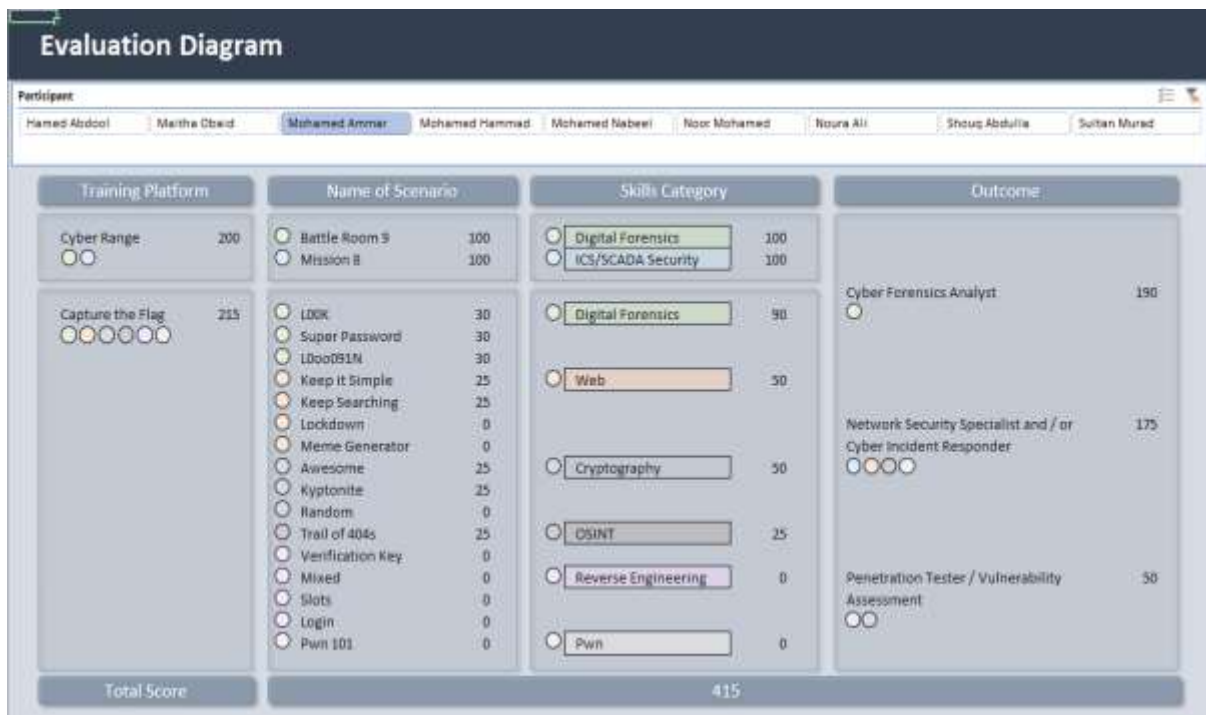


Figure 58: Participant 2 Training Platform Scores and Outcomes

Figure 58 depicts the training platform scores and outcomes for participant 2. As earlier shown the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, he secured 215 points for capture the flag (CTF) challenges. This concluded that the participant acquired great set of hands-on technical skills executing these various 10 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify him to fill in technical roles such as cyber forensics analyst, a network security specialist/Cyber incident responder, and penetration tester/vulnerability assessment.

5.5.3 Participant 3 Skills Performance Evaluation

Participant 3, is a male 4th-year student who majored in Applied Bachelor in Information Security (specialization of Secure Software Development) with excellent

academic status, secured 3.5 GPA and is studying at Abu Dhabi Polytechnic Institute. The participant scored well amongst other participants in the study as he was able to complete a total of 6 scenarios. He scored a completion rate of 33.3%. He was able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, web security, and OSINT. His playing time in battle room 9 was 19hours and mission 8 1hour. The number of times participant 3 played battle room 9 was 3 times and mission 8 was 3 times. Figure 59 depicts the Participant 3 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist/cyber incident responder related tasks, and 130 points in cyber forensics analyst related tasks.



Figure 59: Participant 3 Cybersecurity Skills Performance Level



Figure 60: Participant 3 Training Platform Scores and Outcomes

Figure 60 depicts the training platform scores and outcomes for participant 3. As earlier shown the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, he secured 105 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing these various 6 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify him to fill in technical roles such as cyber forensics analyst, and a network security specialist/Cyber incident responder.

5.5.4 Participant 4 Skills Performance Evaluation

Participant 4, is a female 4th-year student who majored in Bachelors of Science in Information Security with excellent academic status, secured 3.1 GPA and is studying at Zayed University. The participant scored well amongst other participants in the study as

she was able to complete a total of 7 scenarios. She scored a completion rate of 38.9%. She was also able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, web security, and OSINT. Her playing time in battle room 9 was 23hours and mission 8 2hour. The number of times participant 4 played battle room 9 was 5 times and mission 8 was 7 times. Figure 61 depicts the Participant 5 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist/cyber incident responder related tasks, 130 points in cyber forensics analyst related tasks and 25 in penetration tester/vulnerability assessment.

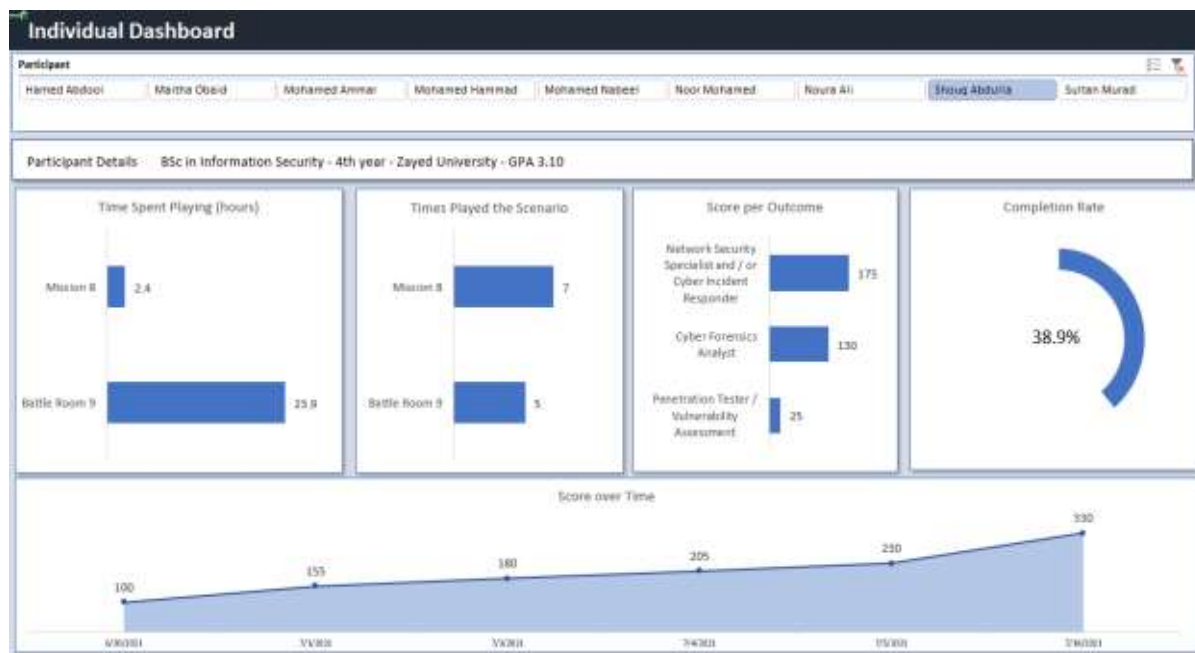


Figure 61: Participant 4 Cybersecurity Skills Performance Level

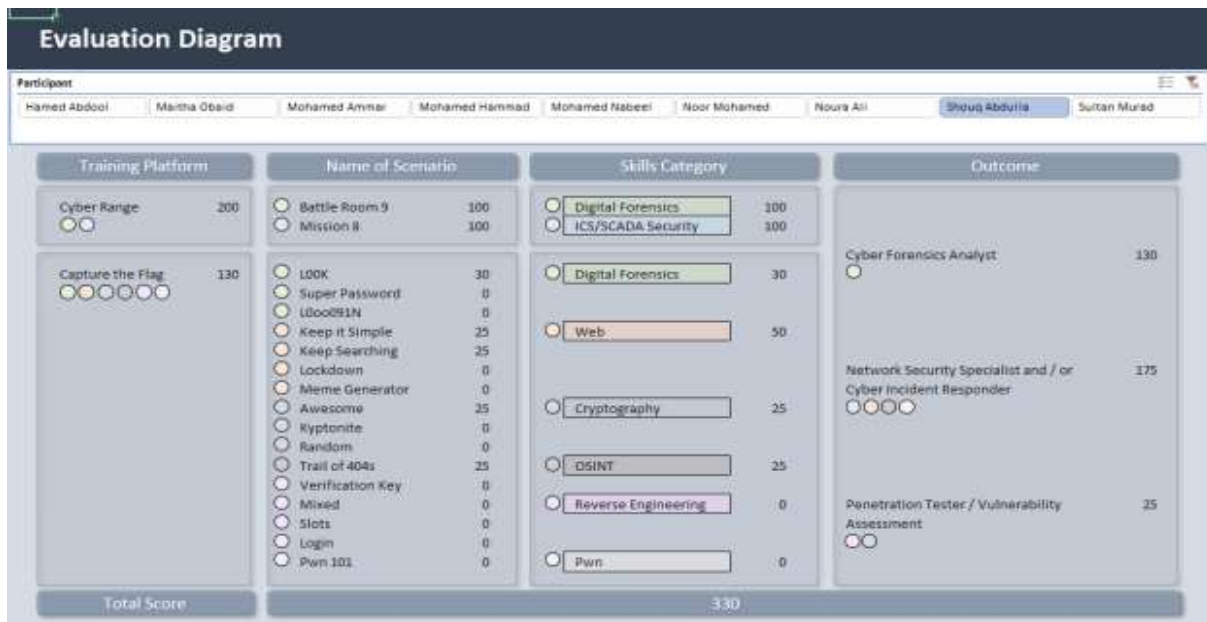


Figure 62: Participant 4 Training Platform Scores and Outcomes

Figure 62 depicts the training platform scores and outcomes for participant 4. As earlier shown, the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, she secured 130 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing the various 7 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify her to fill in technical roles such as cyber forensics analyst, a network security specialist/Cyber incident responder, and a penetration tester/vulnerability assessment.

5.5.5 Participant 5 Skills Performance Evaluation

Participant 5, is a female 4th-year student who majored in Bachelors of Science in Information Security with excellent academic status, secured 3.9 GPA and is studying at Zayed University. The participant scored well amongst other participants in the study as she was able to complete a total of 7 scenarios. She scored a completion rate of 38.9%.

She was also able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, web security, and OSINT. Her playing time of battle room 9 was 14hours and mission 8 2hour. The number of times participant 4 played battle room 9 was 4 times and mission 8 was 9 times. Figure 63 depicts the Participant 5 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist / cyber incident responder related tasks,130 points in cyber forensics analyst related tasks and 25 in penetration tester/vulnerability assessment.

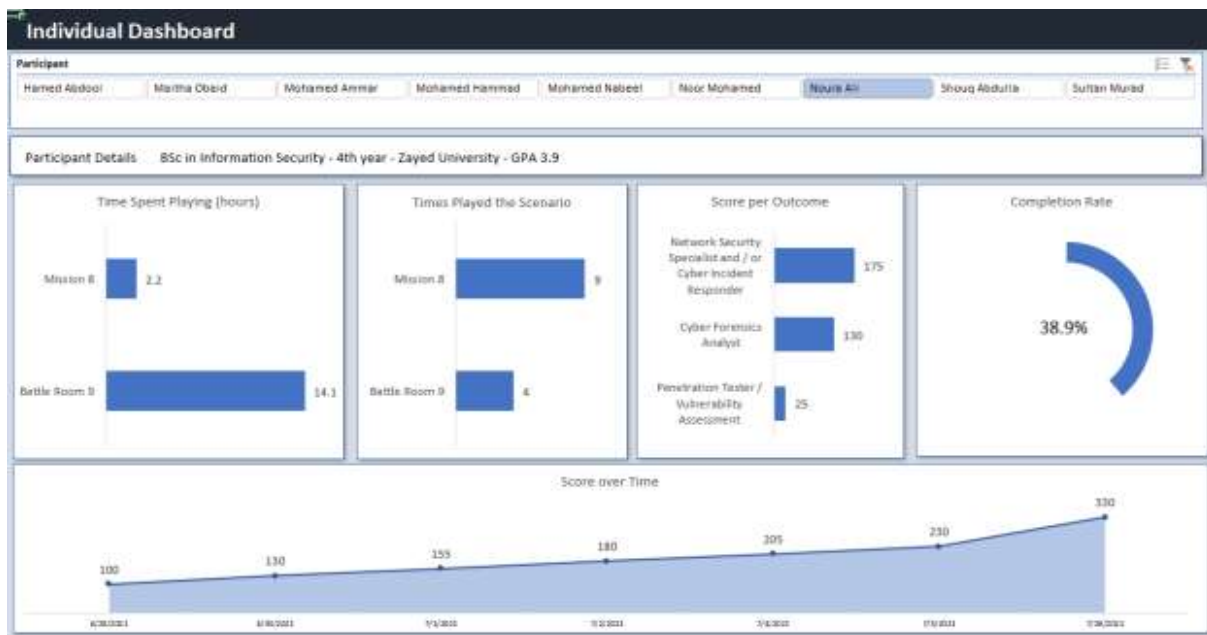


Figure 63: Participant 5 Cybersecurity Skills Performance Level

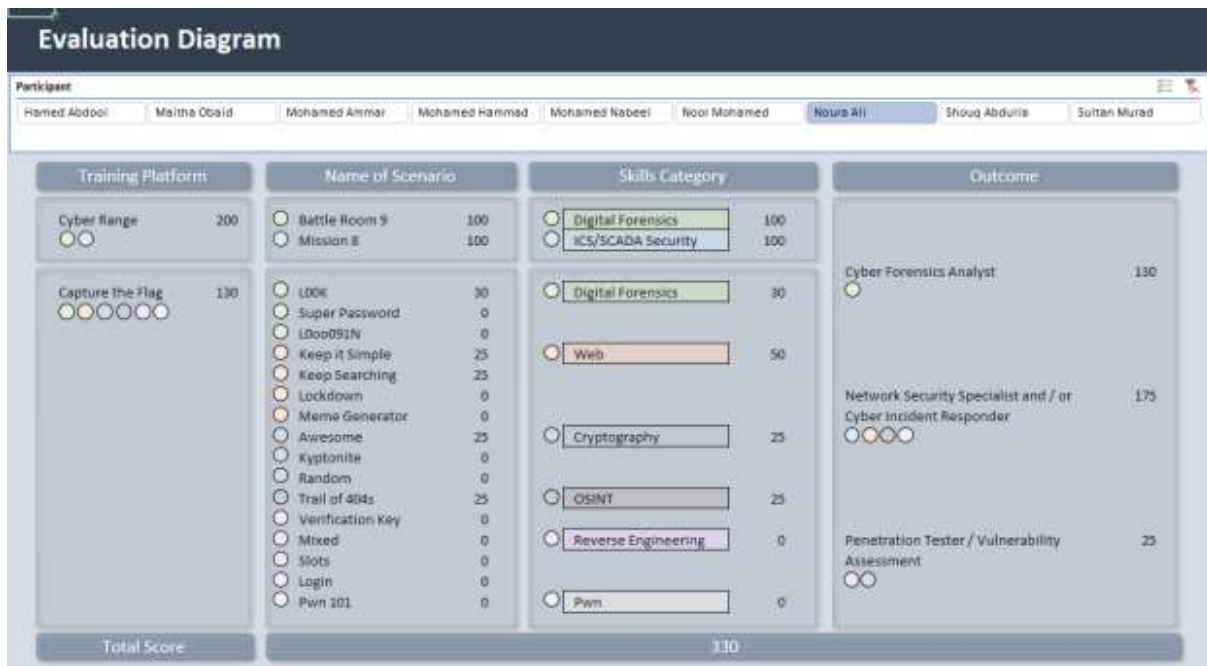


Figure 64: Participant 5 Training Platform Scores and Outcomes

Figure 64, depicts the training platform scores and outcomes for participant 5. As earlier shown, the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, she secured 130 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing the various 7 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify her to fill in technical roles such as cyber forensics analyst, a network security specialist/Cyber incident responder, and a penetration tester/vulnerability assessment.

5.5.6 Participant 6 Skills Performance Evaluation

Participant 6, is a female 3rd-year student who majored in Bachelors of Science in Information Security with excellent academic status, secured 3.86 GPA and is studying at Zayed University. The participant scored well amongst other participants in the study

as she was able to complete a total of 7 scenarios. She scored a completion rate of 38.9%. She was also able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, web security, and OSINT. Her playing time in battle room 9 was 21 hours and mission 8 2 hour. The number of times participant 4 played battle room 9 was 6 times and mission 8 was 10 times. Figure 65 depicts the Participant 6 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist/cyber incident responder related tasks, 130 points in cyber forensics analyst related tasks and 25 in penetration tester/vulnerability assessment.

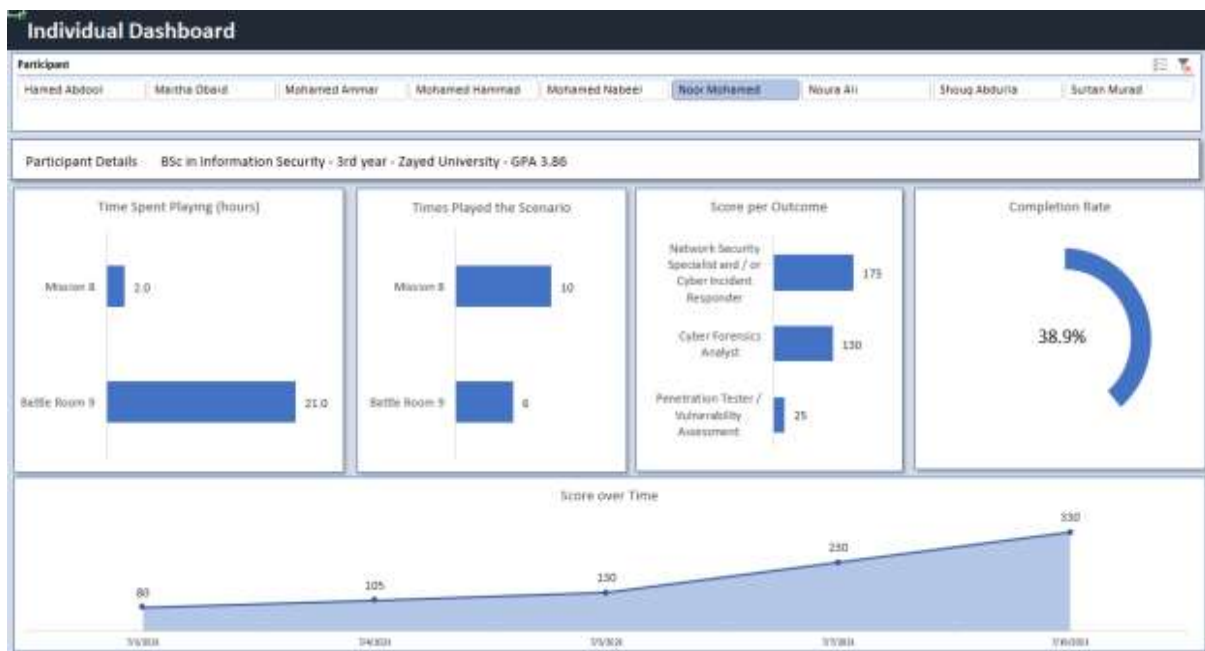


Figure 65: Participant 6 Cybersecurity Skills Performance Level

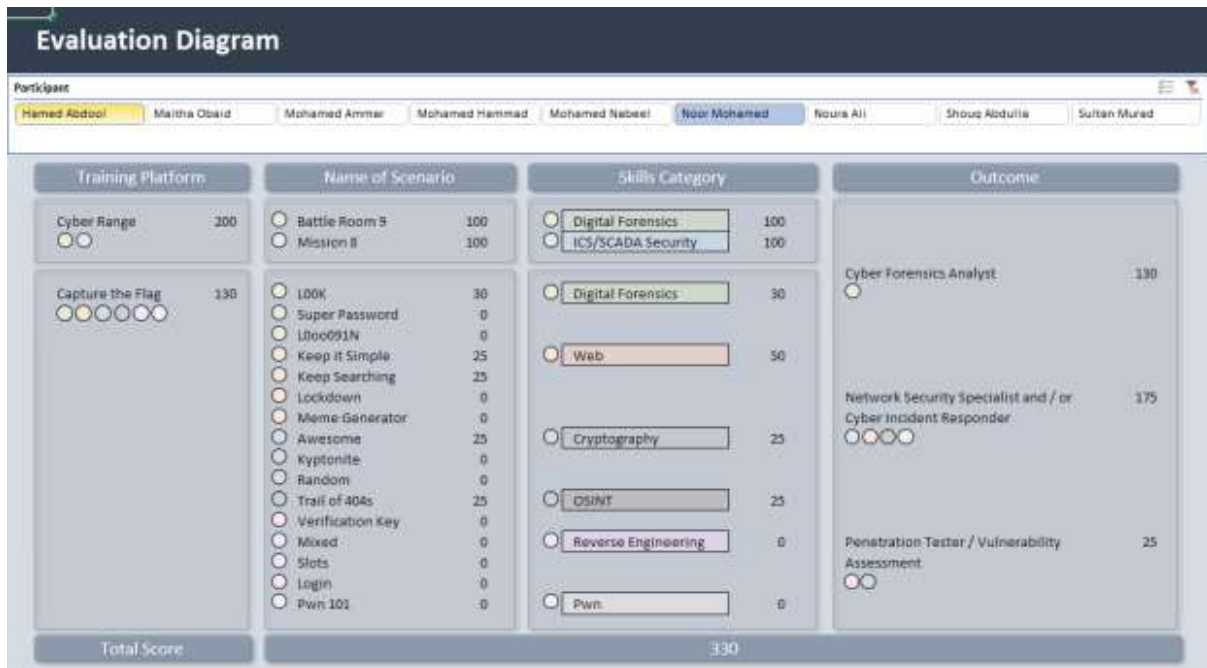


Figure 66: Participant 6 Training Platform Scores and Outcomes

Figure 66 depicts the training platform scores and outcomes for participant 6. As earlier shown, the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, she secured 130 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing the various 7 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify her to fill in technical roles such as cyber forensics analyst, a network security specialist/Cyber incident responder, and a penetration tester/vulnerability assessment.

5.5.7 Participant 7 Skills Performance Evaluation

Participant 7, is a female 4th-year student who majored in Bachelors of Science in Computer Engineering with excellent academic status, secured 3.78 GPA and is studying at Khalifa University. The participant scored well amongst other participants in the study

as she was able to complete a total of 7 scenarios. She scored a completion rate of 38.9%. She was also able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, cryptography, web security, and OSINT. Her playing time in battle room 9 was 16hours and mission 8 21hours. The number of times participant 4 played battle room 9 was 2 times and mission 8 was 13 times. Figure 67 depicts the Participant 7 Cybersecurity Skills Performance level. The participant secured 175 points in network security specialist/cyber incident responder related tasks, 130 points in cyber forensics analyst related tasks and 25 in penetration tester/vulnerability assessment.

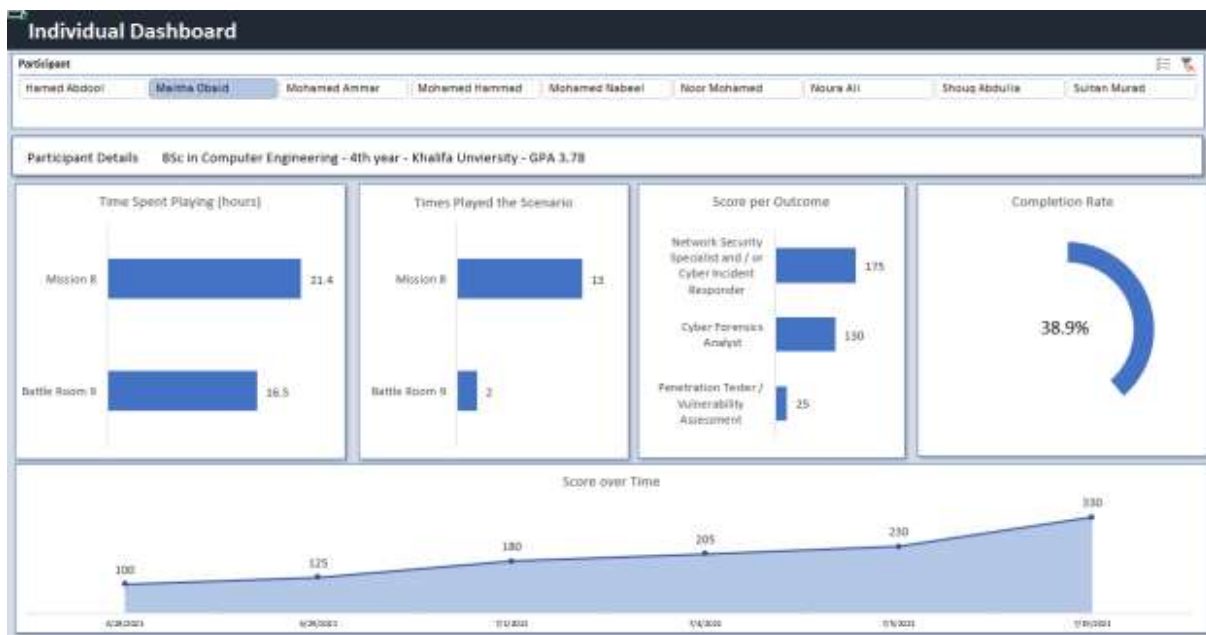


Figure 67: Participant 7 Cybersecurity Skills Performance Level

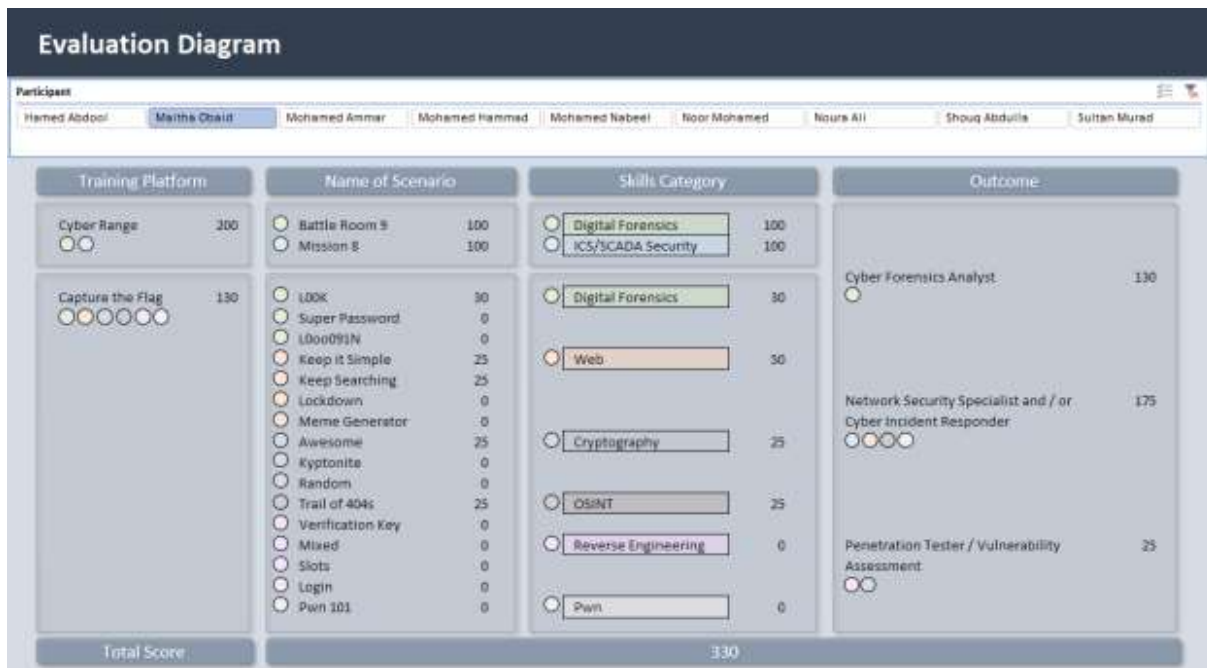


Figure 68: Participant 7 Training Platform Scores and Outcomes

Figure 68 depicts the training platform scores and outcomes for participant 7. As earlier shown, the participant secured 200 points in digital forensics and ICS/SCADA security training for the cyber range platform. Also, she secured 130 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing the various 7 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify her to fill in technical roles such as cyber forensics analyst, a network security specialist/Cyber incident responder, and a penetration tester/vulnerability assessment.

5.5.8 Participant 8 Skills Performance Evaluation

Participant 8, is a male 4th-year student who majored in Bachelors of Science in Information Security with excellent academic status, secured 3.64 GPA and is studying at Zayed University. The participant scored well amongst other participants in the study

as he was able to complete a total of 6 scenarios. He scored a completion rate of 33.3%. He was able to complete both the battle room 9 and mission 8 scenarios on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, web security, and OSINT. His playing time in battle room 9 was 20hours and mission 8 was 1hour. The number of times participant 3 played battle room 9 was 4 times and mission 8 was 3 times. Figure 69 depicts the Participant 8 Cybersecurity Skills Performance level. The participant secured 150 points in network security specialist/cyber incident responder related tasks, 130 points in cyber forensics analyst related tasks, and 25 in penetration tester/vulnerability assessment.

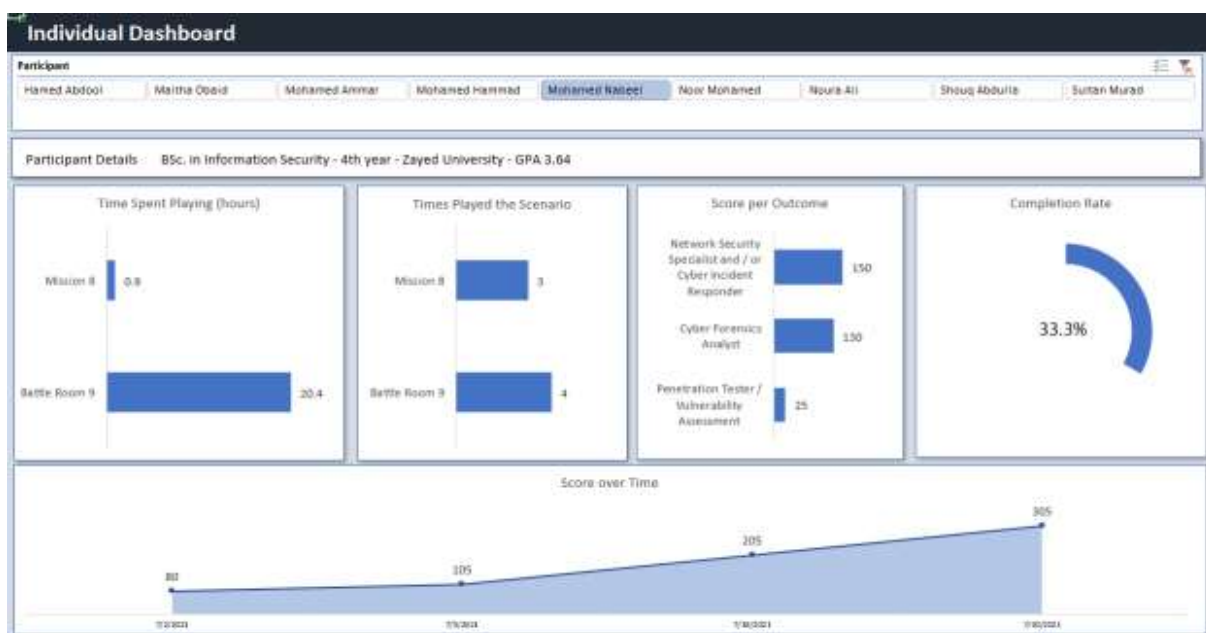


Figure 69: Participant 8 Cybersecurity Skills Performance Level

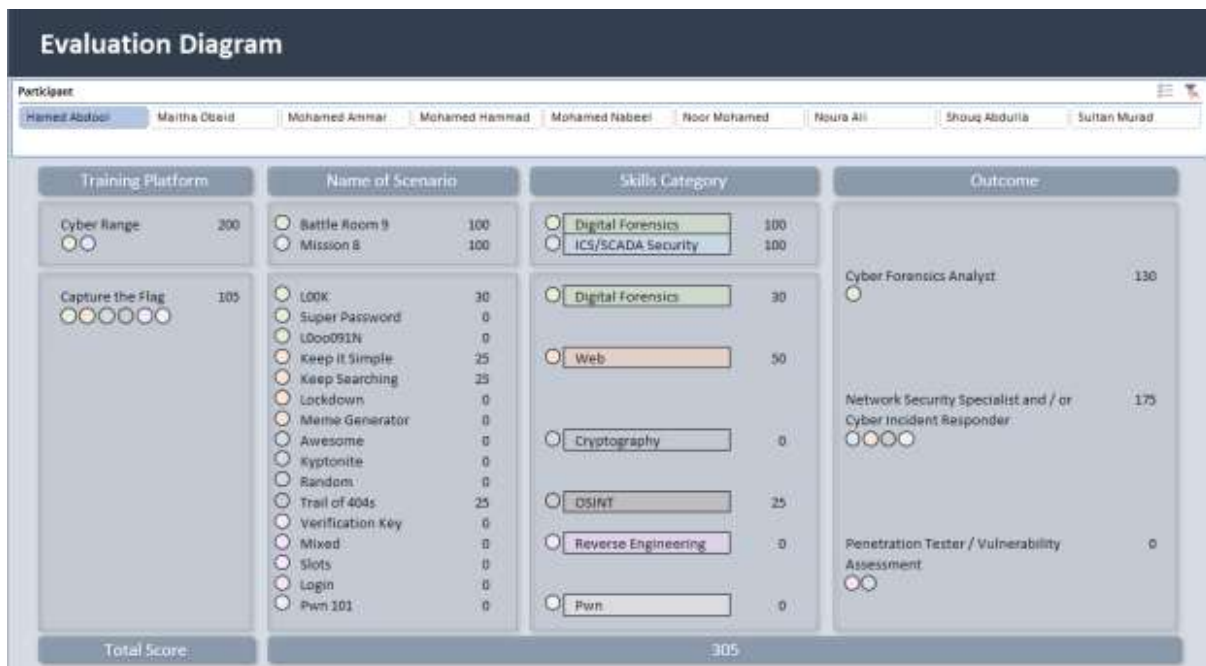


Figure 70: Participant 8 Training Platform Scores and Outcomes

Figure 70 depicts the training platform scores and outcomes for participant 8. As earlier shown, the participant secured 200 points in digital forensics and ICS / SCADA security training for the cyber range platform. Also, he secured 105 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing these various 6 challenges on both platforms. Based on the technical skills acquired it indicates that the participant possesses technical skills that qualify him to fill in technical roles such as cyber forensics analyst, and a network security specialist/Cyber incident responder.

5.5.9 Participant 9 Skills Performance Evaluation

Participant 9, is a male 3rd-year student who majored in Bachelors of Science in Information Security with excellent academic status, secured 3.9 GPA and is studying at Higher Colleges of Technology. The participant scored well amongst other participants in

the study as he was able to complete a total of 5 scenarios. He scored a completion rate of 27.8%. He was able to complete battle room 9 scenario on the cyber range platform and completed various scenarios on the capture the flag platform in the areas of digital forensics, web security, and OSINT. His playing time in battle room 9 was 15hours. The number of times participant 9 played battle room 9 was 11 times. Figure 71 depicts the Participant 9 Cybersecurity Skills Performance level. The participant secured 75 points in network security specialist/cyber incident responder related tasks, and 130 points in cyber forensics analyst related tasks

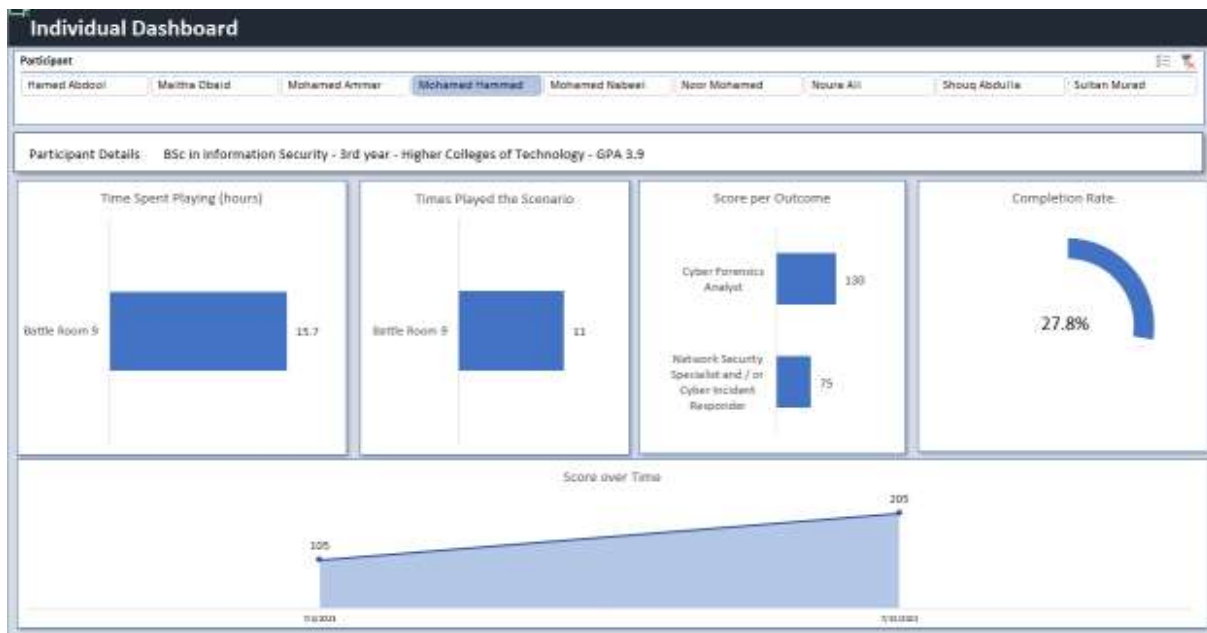


Figure 71: Participant 9 Cybersecurity Skills Performance Level

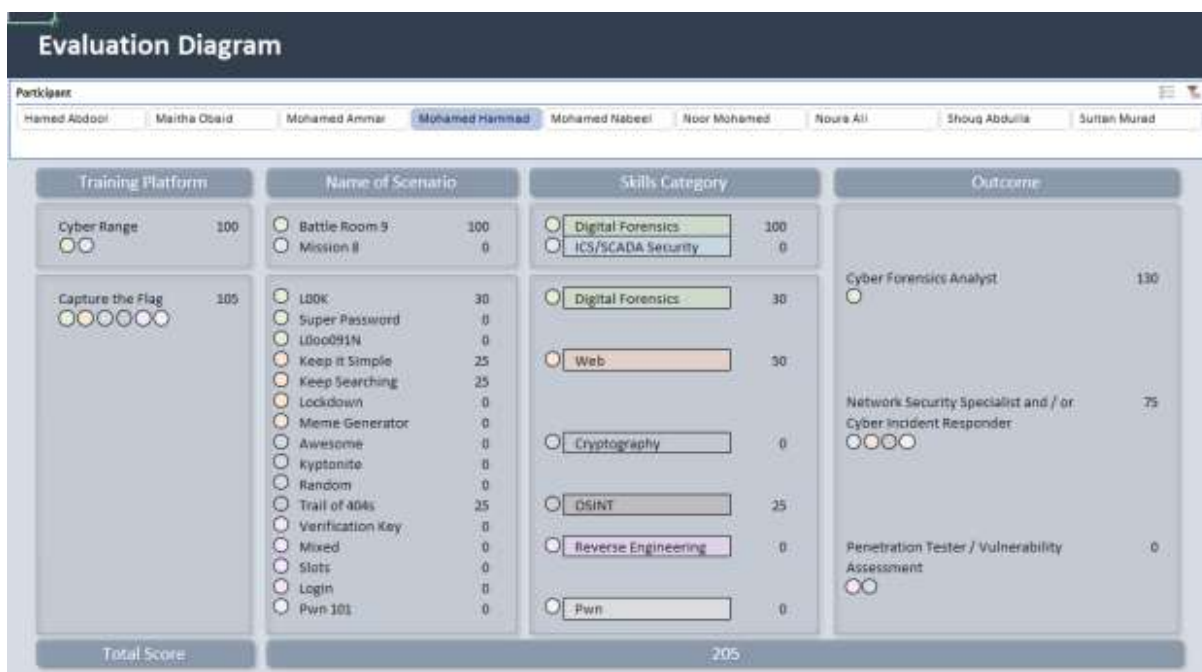


Figure 72: Participant 9 Training Platform Scores and Outcomes

Figure 72 depicts the training platform scores and outcomes for participant 9. As earlier shown, the participant secured 100 points in digital forensics training for the cyber range platform. Also, he secured 105 points for capture the flag (CTF) challenges. This concluded that the participant acquired good set of hands-on technical skills executing these various 5 challenges on both platforms. Based on the technical skills acquired it indicates that the participants possess technical skills that qualify him to fill in technical roles such as cyber forensics analyst, and a network security specialist/Cyber incident responder.

Appendix 8 thoroughly presents the participants' skills performance data captured from the cybersecurity skills performance dashboard (CSPD).

5.6 Summary

In this chapter the design and development of the cybersecurity skills performance dashboard application was thoroughly discussed. The chapter also explained the importance of a nationwide skills performance dashboard to provide true assessment of the available hands-on technical skills and those that need to be further trained and developed. As currently there exists no such cybersecurity skills performance dashboard in the United Arab Emirates that can provide such kind of information to be able to make informed decision on what initiatives and campaigns need to take place in order to build capacity amongst cybersecurity professionals. To that end, this skills performance dashboard acts as a contribution to this research work that can be utilized by policymakers, businesses, education sectors, and cybersecurity professionals.

Next, chapter 6 provides conclusion and recommendations for future research and discusses the findings in further precise details.

6. CONCLUSION, FINDINGS, AND RECOMMENDATIONS

The purpose of this qualitative grounded theory research was to design and develop the cybersecurity skills performance dashboard (CSPD) to display and measure the hands-on technical skills of undergraduate students majored in cybersecurity through understanding and exploring the use of the technical gamification simulation platform (TGSP) to enhance and upscale the technical skills.

The qualitative experiment program focused on identifying new effective ways to be introduced alongside undergraduate cybersecurity academic programs to enable effective hands-on technical skills outcomes amongst undergraduate students.

This chapter of the thesis will present a summary of key research findings, recommendations, contribution to knowledge, research implications and threats to validity, and recommendations for future research work. This research work is of high importance as the requirement to supply superior cluster of cybersecurity professionals who are skilled and technically proficient is increasing as highlighted in the literature review of this thesis. Hence, there is a significant need for educational sectors to evolve their current undergraduate cybersecurity academic programs to produce skilled and technically proficient cybersecurity professionals.

To reiterate the latest study by (ISC, 2020) shows a staggering shortage of 3.1 million cybersecurity professionals around the globe. The gap is most significant in Asia with a shortage of 2 million individuals, followed by a shortage of 527,000 professionals in Latin America, 376,000 professionals in North America and 168,000 in Europe.

6.1 Key Research Findings

The purpose of this qualitative grounded theory research was to understand and explore how the use of the technical gamification simulation platform is used to enhance the hands-on technical skills of undergraduate students who majored in cybersecurity. The significance of this study is to design and develop the cybersecurity skills performance dashboard (CSPD) to display and measure the enhancement of the hands-on technical skills of undergraduate students majored in cybersecurity. In addition to, introducing new ways of instructing undergraduate cybersecurity academic program to produce skills and technically proficient cybersecurity professionals. The research question addressed by this study was

Can the use of the technical gamification simulation platform (TGSP) upscale the hands-on technical skills amongst cybersecurity undergraduate students?

The research was able to conduct an experiment program that was structured in three phases to meet the research objectives of this study. The three phases were assess, train and perform. At every phase of the experiment, data was collected and analyzed immediately to reach the state of saturation regarding the experiences, views and reflections shared by the participants in the study. Once the research experiment was concluded, several research questions were addressed and answered as follows:

- *Research Question 1 of this study was: What are the student's hands-on technical skills experiences once they complete their 4th-year cybersecurity undergraduate degree program?*

The first phase of the experiment program is known as the assessment phase, where the participants are on boarded to the experiment program and do not have access to the training platform. At this phase, the researcher conducted one-on-one interviews with the participants, and the responses shared by the participants enabled the researcher to address this question. As per Chapter 5 of this thesis, the findings indicated that the current state assessment of the 4th-year participants' hands-on technical skills is poor and needs to be significantly developed.

- *Research Question 2 of this study was: What are the student's hands-on technical skills experiences once they complete the cyber range gamification platform scenarios (i.e., both Battle Rooms and Missions)?*

The third phase of the experiment program is the performance phase. The researcher extracted the raw data from the cyber range administrative panel and fed it into the cybersecurity skills performance dashboard application that the researcher developed. The findings from the dashboard application indicated that all the 9 participants were able to complete both the scenarios on the cyber range platform that is battle room 9 (a digital forensics scenario) and mission 8 (an ICS/SCADA network security and incident response scenario). Furthermore, the participants spend between 15-20hours playing the scenarios and have completed the scenarios more than 3 times. This indicates that the participants have not only acquired new hands-on technical skills but are continuing to hone their skills through re-executing the scenarios multiple times.

- *Research Question 3 of this study was: What are the student's hands-on technical skills experiences once they complete the capture the flag gamification platform scenarios?*

As mentioned above, the third phase of the experiment program that is the performance phase is when data from capture the flag platform was extracted and fed into the researcher developed skills performance dashboard application. The findings for capture the flag developed hands-on technical skills were that it was unlike cyber range where all participants were able to complete the scenarios. In the capture the flag platform, every participant had a different experience with CTF platform.

Some participants completed 13 scenarios on the CTF and some completed only 6 scenarios. Findings indicated that CTF platform is different from the CR platform where the latter is a learning and testing tool by providing hints. However, the CTF is only considered an assessment tool of the hands-on technical skills. Any skills that the participant does not possess, he/she needs to search the Internet. Build the skill and then complete the scenario in the CTF platform. The dashboard findings indicated that participants in the study acquired various skills ranging from digital forensics, to cryptography, web security, reverse engineering, pwn, and OSINT.

- *Research Question 4 of this study was: What are the student's experiences on the effective training platform considering the cyber range and / or capture the flag?*

Once the experiment program was concluded, the participants filled in a post-train survey questionnaire where the responses from the questionnaire was analyzed. Findings indicated that most participants appreciated both the platforms as they both led them to gain new technical skills and helped them improve the ones they had before. Furthermore, findings indicated that participants appreciated CTF more than CR because

it provided a variety of domains to practice such as digital forensics, cryptography, web security, pwn, OSINT, amongst others.

In addition, the difficulty level to complete these challenges range from beginner to intermediate to advanced, hence, providing participants with the difficulty level they desire. Nevertheless, findings also indicated participants preferred cyber range platform as there was a structure to solving a scenario about one specific simulated real-world environment. In addition, the learning curve was higher in the cyber range platform compared to capture the flag.

- *Research Question 5 of this study was: How can the hands-on technical skills acquired by the students using the technical gamification simulation platform can be validated using the dashboard?*

This was addressed by the researcher by designing and developing the cybersecurity skills performance dashboard to validate the findings from the experiment program and to act as a contribution to this research work. Thorough details about the design and development of the skills performance dashboard application are in Chapter 4. It has shown explicitly that the dashboard was developed and designed in order to validate the use of the gamification platforms as means to improve the hands-on technical skills of the participants of the experiment.

6.2 Recommendations

Once the research was completed, various recommendations emerged that can serve various stakeholders in regards to the findings presented in this research work, such as:

- Cybersecurity professionals need to continue honing their current hands-on technical skills and progressively acquire new ones to be better able to safeguard the businesses they serve and be ahead of their cyber adversaries as the cyber threat landscape is rapidly evolving.
- The educational sector needs to make significant efforts to introduce new ways of instructing the undergraduate cybersecurity academic programs by integrating technical gamification simulation platforms to produce market ready skilled and technically proficient cybersecurity professionals.
- Policymakers need to understand by using the cybersecurity skills performance dashboard application, the currently available technical skills and those that are not available to make informed decisions on the home-grown initiatives and campaigns that need to be invested in to train and develop the non-existent technical skills.
- Businesses need to use the cybersecurity skills performance dashboard application to better choose the cybersecurity practitioner that they require in terms of the technical skills that the practitioner exhibits. This will save businesses the time and the money to identify a candidate and fill in the role.
- Cybersecurity professionals need to use the cybersecurity skills performance dashboard application so as for it to serve as a credible source of the technical skills that they have. In addition, viewing the leaderboard of cybersecurity professionals with wide range of skills will motivate them to gain and develop their technical skills even further.

- Public and private sectors need to understand the significance of these technical gamification simulation platforms and ensure that they can invest in and provide it as a national resource for the students or make it available to train and develop their internal cybersecurity team.

6.3 Contribution to Knowledge

To the best of the researcher's knowledge, this research work is considered to be the first to be conducted in the United Arab Emirates that examined providing undergraduate students majoring in cybersecurity with access to the technical gamification simulation platform for a duration of 8-weeks for the purpose of understanding and exploring how the platform will upscale their hands-on technical skills. Hence, this is considered as a contribution to the previous literature work. Furthermore, this research provided two different training platforms to be better able to present findings and results as contribution to the body of knowledge. Being the first to have been conducted, this research can be used as a base for any other progressive research that can tackle other areas such as high school students, or mapping the dashboard to the NIST/ADDA work roles assessment tool.

In addition, as a contribution to computer science, the researcher designed and developed a cybersecurity skills performance dashboard application that can act as a nationwide performance dashboard to serve the various stakeholders such as educational sectors, business owners, policymakers, cybersecurity professionals, and public & private sectors. Other business dashboard applications can be built on this concept of providing a true assessment of the skill and talents available and the ones that need to be developed.

6.4 Usability of the Dashboard to the Industry

The dashboard is considered a tool that the cyber security industry use in many ways. The usability of the dashboard to the industry is listed as follows:

1. Public and Private Sector can use the dashboard to either search and hunt for cyber security professionals that possess specific technical skills that is required. Or can use the tool in order to advertise active cyber security job postings so that the cyber security professionals can apply based on the skills required;
2. The UAE cyber security council can use the dashboard to know for sure what is the actual skills gap that is evident and what are the various skills that needs to be built amongst the cyber security professionals;
3. The educational institutions can use the dashboard in order to gain insight on the effectiveness of their cyber security academic programs and understand how to better improve the programs in future;
4. The professional certification institutions can use the tool to understand what are the cyber security skills that are missing or lacking and how can they develop the required courses to bridge the skills gap;
5. The local security authorities can use the dashboard to better tailor their capacity building programs and the effectiveness of their capacity building programs; and
6. Cyber security professionals can use the dashboard to view the progress of their technical skills and the dashboard can act as a credible platform to validate their technical skills.

6.5 Research Implication

Although this research study captured a sample size of participants who are UAE nationals and from specific universities in the UAE, the research findings can still be generalized and relied upon to be true to any nationality within the UAE or globally and is true to be applied for any education institution regardless it is governmental or private. The thoroughness of the experiment program and approach of data collection and analysis at every phase of the experiment ensures the research validity.

The research's findings have implications for improving the undergraduate cybersecurity academic program by integrating the technical gamification simulation platform to enable the educational institutions to produce cybersecurity professionals and this can be applied not only in the UAE but even globally to shorten the skills gap problem. The policymakers can further enhance and work upon the research by covering a larger sample for the research that can include even high school students. Furthermore, the skills performance dashboard can further be developed to include different domains and to map it to the ADDA or aeCERT cybersecurity roles and required knowledge, skills, and abilities.

The results of this research can be added to the body of research literature on cybersecurity skills training and workforce development as well as serve all other sectors that need to benefit from the skills performance dashboard.

6.6 Threats to Validity

Every research study is prone to certain threats to validity, an inevitable fact in any research world. This section will present the threats to validity of this research work. the lack of literature that tackles the problem of evolving the traditional cybersecurity

academic curriculum to produce market-ready cybersecurity professionals was one of the major threats to validity of this research work. This problem was echoed thoroughly and discussed in the literature review of this thesis. The researcher took significant interest to fill this gap by introducing the technical gamification simulation platform that consists of two different training platforms, that is the cyber range platform and the capture the flag platform and ensured that a well-structured experiment program is in place for the participants in the study to go through. Although both training platforms upscale the hands-on technical skills amongst the participants, they are however, different in their approach.

Another threats to validity to this research work is that the sample size was supposed to be 10 participants. However, in the midst of the experiment program, one of the participants fell sick and had to withdraw from the program, leaving it to only 9 participants. Nevertheless, the researcher ensured that the shrink in the sample size of the study did not negatively impact data collected, results, or the conclusion.

A final threat to validity was that although capture the flag platform was publicly available for the participants to execute and complete as many challenges as possible, the cyber range platform was a commercial software license with paid subscription to the various battle rooms and missions hosted on the platform. Hence, the researcher was only able to provide the participants in the study with two distinct scenarios of battle room 9 and mission 8. Although this threat to validity was present, the researcher ensured that the experiment was structured in a way that the participants would have access to both training environments of varying difficulty level of simulated real-world environment for both a cybersecurity environment and an operational technology environment.

6.7 Future Works

The research findings indicated a strong interest of participants in the concept of having access to the technical gamification simulation platform. Hence, if the students have a strong interest, then educational institutions need to evolve to include this new way of instruction to produce skilled and technically proficient cybersecurity professionals. An empirical study needs to be conducted to measure the rise in the hands-on technical skills if a university offers the CTF as part of the coursework for 3rd or 4th-year students to measure the interest of students and willingness to complete and work on the scenarios.

In addition, the researcher urges that this study be conducted again with a larger sample of participants from different universities and different mindsets to understand if there are any additional findings that were not noted by this research work. Furthermore, this research work had limited access to cyber range scenarios, it would be great to work on a research work that has wider selection of scenarios for the participants to have access to and learn any new findings that evolve. The researcher recommends that future work can consider a sample from year 1 or 2 of the undergraduate program or high school students to explore any new findings to this research. Furthermore, the researcher urges work on the skills performance dashboard on other fields of data that can be fed to the application and the data that can be presented to be of help and use by other stakeholders.

6.8 Conclusion

To conclude, this research study presented the design and development of the cybersecurity skills performance dashboard to display and measure the upscale in the hands-on technical skills amongst the undergraduate university students majored in

cybersecurity. In addition, the study examined the use of technical gamification simulation platform to upscale the hands-on technical skills amongst the undergraduate students.

This study started with an examination of the literature, which eventually led to the identification of the gap and hence the development of the problem and purpose statement. The general problem was that there is a staggering shortage of 3.1 million cybersecurity professionals around the globe (ISC, 2020) and the industry needs a sufficient supply of skilled and technically proficient cybersecurity professionals.

The specific problem was that the current undergraduate cybersecurity academic program does not produce market ready cybersecurity professionals and the need was to find new ways to introduce into the academic program that can enable them to produce skilled and technically proficient cybersecurity professionals.

Hence, the purpose of this qualitative grounded theory research study was to design and develop the cybersecurity skills performance dashboard (CSPD) to display and measure the enhancement in the hands-on technical skills of undergraduate students majored in cybersecurity through understanding and exploring the use of the technical gamification simulation platform (TGSP) to enhance and upscale the technical skills.

The research conducted a well-structured 8-weeks long experiment program examining the experiences, views, and reflections of 3rd and 4th-year undergraduate students by providing them access to two types of training platforms that is the cyber range platform and the capture the flag platform.

The findings indicated an increased level of enhancement in the hands-on technical skills of all the participants in the study as presented by the cybersecurity skills performance dashboard (CSPD) designed and developed by the researcher.

Finally, this research work achieved the research objectives set and answered all the research questions based on the findings from the study. The study concluded with setting the path for future works.

REFERENCES

- Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence Issue and Challenges . *Indonesian Journal of Electrical Engineering and Computer Science* , 10(1), 371-379.
- Abu-Taieh, E., Faries, A. A., AlOtaibi, S., & Aldehim, G. (2018). *Cybersecurity Body of Knowledge and Curricula Development* . DOI:10.5772/intechopen.77975.
- ADDA. (2021). *Cybersecurity Guidelines*. Abu Dhabi : Abu Dhabi Digital Authority.
- aeCERT. (2021). *National Cybersecurity Workforce Framework* . UAE: TDRA-aeCERT.
- Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber harms: Defining the impacts of cyber-attacks and understanding how they propagate. . *Journal of Cybersecurity*, 4(1).
- Alfred, N. (2019, January 4). *Marriott says hackers stole more than 5 million passport numbers*. Retrieved from Cnet: <https://www.cnet.com/news/marriott-says-hackers-stole-more-than-5-million-passport-numbers/>
- Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., & Mohammad, A. N. (2020). New insider threat detection method based on recurrent neural networks. *Indonesian Journal of Electrical Engineering and Computer Science*, 17(3), 1474-1479. Retrieved 8 8, 2021, from <http://ijeecs.iaescore.com/index.php/ijeecs/article/view/18801>
- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). *Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis*. Springer.
- Archibald, N. T. (2020). *Cybersecurity and Critical Infrastructure*. Retrieved 8 8, 2021, from <https://ujpps.com/index.php/ujpps/article/view/93>
- Arghire, I. (2019, February 20). *Security Week*. Retrieved from securityweek.com: <https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec>

- Bagley, C. E. (2018). *Managers and the Legal Environment: Strategies for Business*. Boston: Cengage Learning.
- BBC. (2019, 07 26). *Ransomware hits Johannesburg electricity supply*. Retrieved from <https://www.bbc.com/news/technology-49125853>
- Benson, V., McAlaney, J., & Frumkin, L. A. (2019). Emerging Threat for the Human Element and Countermeasures in Current Cyber Security Landscape. *IGI Global, Publisher of Timely Knowledge*.
- BIPSS. (2012). *Cyber Security: The Emerging Threat Landscape*. Dhaka: Bangladesh Institute of Peace and Security Studies.
- Blair, T. (2017). *Investigating the cybersecurity skills gap*. ProQuest Dissertations Publishing.
- Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, 88, 101607. Retrieved 8 8, 2021, from <https://sciencedirect.com/science/article/pii/S0167404819301580>
- Brown, S. (2018). *Software Architecture for Developers*. Victoria, BC, Canada: Leanpub.
- Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills*. ProQuest Dissertations Publishing.
- Carnovale, S., & Yeniyurt, S. (2021). *Cyber Security and Supply Chain Management: Risks, Challenges and Solutions*. Portland State: World Scientific Publishing Company.
- Caulkins, B., Marlowe, T., & Reardon, A. (2018). *Cybersecurity Skills to Address Today's Threats*. Springer.
- Caulkins, B., Marlowe, T., & Reardon, A. (2018). *Cybersecurity Skills to Address Today's Threats*. Springer.

- Center for Strategic and International Studies (CSIS) . (2016, July). *CSIS, Hacking the Skills Shortage* . Retrieved from McAfee : <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf>
- Center for Strategic and International Studies. (2016). *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*. VOCED plus.
- Charmaz, K., & Henwood, K. (2017). *Grounded Theory Methods for Qualitative Psychology, 2nd Ed.* . SAGE .
- Charters, E. (2003). The Use of Think-aloud Methods in Qualitative Research: An Introduction to Think-aloud Methods . *Brock Education* , 1-15.
- Chavis, J. S., & Syed, D. P. (2020). *Envisioning Cybersecurity Analytics for the Internet of Things*. 2020 IEEE 3rd 5G World Forum (5GWF).
- Chouliaras, N., Kittes, G., Kantzavelou, I., & Maglaras, L. (2021). *Cyber ranges and testbeds for education, training, and research*. MDPI.
- Cobb, M. J. (2018). *Plugging the skills gap: The vital role that women should play in cybersecurity*. Elsevier.
- Collier, K. (2020, May 22). *Four states warn unemployment benefits applicants about data leaks*. Retrieved from NBC News: <https://www.nbcnews.com/tech/security/four-states-warn-unemployment-benefits-applicants-about-data-leaks-n1212431>
- Constantin, L. (2020, December 10). *FireEye breach explained: How worried should you be?* Retrieved from CSO Online: <https://www.csoonline.com/article/3600893/fireeye-breach-explained-how-worried-should-you-be.html>
- Coolican, H. (2017). *Research Methods and Statistics in Psychology* .
- Creswell, J., & Creswell, D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Pearson Education.

- Creswell, J., & Guetterman, T. (2019). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 6th Edition* . New York, NY : Pearson Education .
- Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap*. JSTOR.
- Cyberbit. (2018). *The State of Cybersecurity Talent*. Cyberbit.
- Cybersecurity Ventures. (2019, October). *Cybersecurity Ventures*. Retrieved from Cybersecurity Talent Crunch to create 3.5 million unfilled jobs globally by 2021: <https://cybersecurityventures.com/jobs/>
- CyberSeek. (2019). *Cybersecurity Supply/Demand Heat Map* . Retrieved from CyberSeek: <https://www.cyberseek.org/heatmap.html>
- Damico, T. M. (2009). Cyber Attack Prevention for the Home User: How to Prevent a Cyber Attack. *Inquiries Journal*, 1(11). Retrieved 8 8, 2021, from <http://inquiriesjournal.com/articles/47/cyber-attack-prevention-for-the-home-user-how-to-prevent-a-cyber-attack>
- Danidou, Y. (2020). *Trusted Computing Initiative on the Spectrum of EU Cyber-Security Legal Framework*. Retrieved 8 8, 2021, from https://link.springer.com/chapter/10.1007/978-3-030-25579-4_13
- De Zan, T. (2020). *Future research on the cyber security skills shortage*. Taylor Francis.
- Diachenko, B. (2019). *800+ Million Emails Leaked Online by Email Verification Service*. Security Discover.
- Digital14. (2021). *UAE Threat Landscape* . Abu Dhabi : Digital14.
- Eckerson, W. (2010). *Performance Dashboards: Measuring, Monitoring, and Managing your Business, 2nd Ed.* . Wiley .
- ECSCA '17. (2017). *Proceedings of the 11th European Conference on Software ArchitectureE: Companion Proceedings*. ACM DL Digital Library.
- El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular*

- Communications*, 23, 100214. Retrieved 8 8, 2021, from <https://sciencedirect.com/science/article/pii/S221420961930261x>
- EMSI. (2020, July). *Economic Modeling*. Retrieved from Build (Don't Buy): A Skills-Base Strategy to Solve the Cybersecurity Talent Shortage : <https://www.economicmodeling.com/cybersecurity/>
- ESG - ISSA. (2020). *The Life and Times of Cybersecurity Professionals 2020*. ESG - ISSA.
- ESG Global and ISSA . (2020, July). *ESG Global* . Retrieved from ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020 : https://www.esg-global.com/esg-issa-research-report-2020?utm_campaign=ESG%20Research&utm_source=slider
- ESG ISSA. (2018). *The Life and Times of Cybersecurity Professionals 2018*. ESG ISSA.
- ESG ISSA. (2021). *The Life and Times of Cybersecurity Professionals - 2021*. ISSA.
- ESG-ISSA. (2021). *The Life and Times of Cybersecurity Professionals 2021*. ESG-ISSA.
- Few, S. (2013). *Information Dashboard Design: Displaying Data for at-a-glance monitoring, 2nd Ed.* . Analytics Press.
- Frost & Sullivan . (2017). *Frost & Sullivan 2017 Global Information Security Workforce Study* . Retrieved from I am Cyber Safe : <https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf>
- Fruhlinger, J. (2020, March 9). *Top cybersecurity facts, figures and statistics*. Retrieved from CSO Online: <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>
- Funnel, S., & Bishop, M. (2020). *Addressing cyber security skills: the spectrum, not the silo*. Elsevier.
- Furfaro, A., Pace, P., & Parise, A. (2020). Facing DDoS bandwidth flooding attacks. *Simulation Modelling Practice and Theory*, 98, 101984. Retrieved 8 8, 2021, from <https://sciencedirect.com/science/article/pii/S1569190X19301170>

- Furnel, S., Fischer, P., & Finch, A. (2017). *Can't get the staff? The growing need for cyber-security skills*. Elsevier.
- Gaus, A. (2013). Trolling Attacks and the Need for New Approaches to Privacy Torts. *University of San Francisco Law Review*, 353-376. Retrieved from University of San Francisco Law Review.
- Graham, C. (2017, May 20). *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history*. Retrieved from telegraph.uk: <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>
- Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Retrieved from Wired: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Herjavec. (2021). *2018-2021 Cybersecurity Jobs Report*. Herjavec Group.
- Hunt, T. (2019, 01 17). *The 773 Million Record "Collection #1" Data Breach*. Retrieved from <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>
- Ikeda, S. (2020, April 27). *Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web*. Retrieved from CPO Magazine: <https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-compromised-by-credential-stuffing-sold-on-dark-web/>
- Imran, M., Arif, T., & Shoab, M. (2018). A Statistical and Theoretical Analysis of Cyberthreats and its Impact on Industries. *International Journal of Scientific Research in Computer Science Applications and Management Studies*, 7(5).
- Ionescu, O., Dumitru, V. G., Pricop, E., & Pircalabu, S. (2020). *Innovative Hardware-Based Cybersecurity Solutions*. Retrieved 8 8, 2021, from https://link.springer.com/chapter/10.1007/978-3-030-31328-9_12
- Ipsos MORI. (2021). *UK Government. Labour Market 2021: Findings Report*. Retrieved from Cyber Security Skills in the UK

<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021>

Ipsos MORI. (2021). *UK Government . Retrieved from Cyber Security Skills in the UK Labour Market 2021: findings report :*
<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021>

ISC. (2020). *Cybersecurity Professionals Stand Up to a Pandemic: Cybersecurity Workforce Study*. ISC.

ISC2. (2018, October). *Cybersecurity Skills Shortage Soars*. Retrieved from ISC2 :
https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

ISSA. (2020). *Cyber Securities Guidance Paper*. International Securities Services Association. Retrieved from <https://www.issanet.org/e/10/507-2020-08-04-cyber-paper.html>

Jain, J., & Pal, P. R. (2017). A recent study over cyber security and its elements. *International Journal of Advanced Research in Computer Science* , 8(3), 791-793.

Kam, H. J., Menard, P., & Katerattanakul, P. (2018). *Ethical hacking: Addressing the critical shortage of cybersecurity talent*. AIS.

Kaspersky Lab . (2016). *Lack of Security Talent: An Unexpected Threat to Corporate Cybersafety* . Retrieved from Kaspersky Lab IT Security Risks Special Report Series 2016 :
https://business.kaspersky.com/security_risks_report_lack_of_security_talent/

Khandelwal, S. (2019). *Hacker Breaches Dozens of Sites, Puts 127 New Million Records Up for Sale*. The Hacker N.

Khera, V. (2018). *A study of cybersecurity for telecommunication services concerning smartphone users in Thailand*. Retrieved 8 8, 2021, from <https://researchrepository.murdoch.edu.au/id/eprint/42126>

- Kolb, D. (2015). *Experiential Learning: Experience as the source of Learning and Development*. Pearson Education ISBN:978-0-13-389240-6.
- Korolov, M. (2021, January 12). *What are Supply Chain Attacks, and How to Guard Against Them*. Retrieved from Data Center Knowledge: <https://www.datacenterknowledge.com/security/what-are-supply-chain-attacks-and-how-guard-against-them>
- Kumaran, N., & Lugani, S. (2020, April 17). *Protecting businesses against cyber threats during COVID-19 and beyond*. Retrieved from Google Cloud: <https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>
- Lou, X., & Tellabi, A. (2020). *Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS)*. Retrieved 8 8, 2021, from https://link.springer.com/chapter/10.1007/978-3-030-31328-9_4
- Maennel, K. (2020). *Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises*. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020.
- Maleh, Y., Shojafar, M., Alazab, M., & Y, B. (2021). *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*. Springer.
- Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. . *European Intelligence and Security Informatics Conference (EISIC) - IEEE* , 91-98 .
- McCubbrey, D. S. (2020). *Cybersecurity Penetration Assessments in the Context of a Global Cybersecurity Skills Gap*. ProQuest Dissertations Publishing.
- MIT Technology Review. (2018). *A Cyber-skills shortage means students are being recruited to fight off hackers* . Retrieved from MIT Technology Review : <https://www.technologyreview.com/2018/10/18/139708/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers/>

- Mohasseb, A., Aziz, B., Jung, J., & Lee, J. (2019). *Predicting cybersecurity incidents using machine learning algorithms: a case study of Korean SMEs*. Retrieved 8 8, 2021, from https://researchportal.port.ac.uk/portal/files/13360330/icissp_2019_24_cr_1_.pdf
- Morales, J. (2009). *Russia's New National Security Strategy: Towards a 'Medvedev Doctrine'?* Retrieved 8 8, 2021, from http://realinstitutoelcano.org/wps/wcm/connect/0558db804fb4cfd6a6f7ff8bf7fc5c91/ari135-2009_morales_russia_new_national_security_strategy_medvedev.pdf?mod=ajperes&cacheid=0558db804fb4cfd6a6f7ff8bf7fc5c91
- NICCS . (2021 , March). *A Glossary of Common Cybersecurity Terminology* . Retrieved from National Initiative for Cybersecurity Careers and Studies : <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary>
- Oates, B. J. (2006). *Researching Information Systems and Computing*. London: SAGE.
- O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, 17(2), 187-209. Retrieved 8 8, 2021, from <https://academic.oup.com/jcsl/article-abstract/17/2/187/852785>
- Office of the Press Secretary. (2017, September 13). *Homeland Security*. Retrieved from dhs.gov: <https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01>
- Oltsik, J. (2018). *ESG Research Suggests Cybersecurity Skills Shortage Is Getting Worse*. Enterprise Research Group (ESG).
- Oosthoek, K., & Doerr, C. (2020). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, 34(2), 300-315.
- Ozkaya, E., & Aslaner, M. (2019). *Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches*. Brimingham: Packt Publishing Ltd.

- Patton, M. Q. (2015). *Qualitative Research and Evaluation Methods: Integrating Theory and Practice, 4th Ed.* . Thousand Oaks, CA: SAGE.
- Pearlso, K. E., Saunders, C. S., & Galletta, D. F. (2019). *Managing and Using Information Systems: A Strategic Approach*. Pittsburgh: John Wiley & Sons.
- Petit, J., & Shladover, S. E. (2015). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2), 546-556. Retrieved 8 8, 2021, from <https://ieeexplore.ieee.org/stamp/redirect.jsp?arnumber=/6979/4358928/06899663.pdf>
- Polityuk, P., Vukmanovic, O., & Jewkes, S. (2017, January 18). *Ukraine's power outage was a cyber attack: Ukrenergo*. Retrieved from reuters.com: <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>
- Popkova, E. G., & Gulzat, K. (2019). Contradiction of the Digital Economy: Public well-being vs. Cyber Threats. *Institute of Scientific Communications Conference, Springer*, pp. 112-124 .
- Reffold, K. (2020). *What the market is not telling you about the cyber security skills shortage*. Henry Stewart Publications.
- RiskBased Security. (2020). *2020 Q3 Report - Data Breach Quick View*. RiskBased Security. Retrieved from <https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf>
- Salant, P., & Dillman, D. A. (1994). *How to conduct your own survey*. New York: John Wiley & Sons .
- Sayegh, E. (2020). *As The End Of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse*. Retrieved from Forbes: <https://www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/?sh=d0f8b025f868>

- Schneiderman, R. (2017, September). *Cyber Skills in High Demand Well Into the Future* . Retrieved from Newswise : <https://www.newswise.com/articles/cyber-skills-in-high-demand-well-into-the-future>
- Shires, J. (2018). *Enacting expertise: Ritual and risk in cybersecurity*. Cogitatio Press.
- Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, 41(1), 82-107. Retrieved 8 8, 2021, from <https://tandfonline.com/doi/full/10.1080/13523260.2019.1670006>
- Smart Energy International. (2015, May 20). *Turkey's blackout: Did a cyber attack cause grid outage?* Retrieved from smart-energy.com: <https://www.smart-energy.com/regional-news/africa-middle-east/turkeys-blackout-did-a-cyberattack-cause-grid-outage/>
- Smith, G. (2016). *The intelligent solution: automation, the skills shortage and cyber-security*. Elsevier.
- Sobers, R. (2021, March 16). *134 Cybersecurity Statistics and Trends for 2021*. Retrieved from Varonis: <https://www.varonis.com/blog/cybersecurity-statistics/>
- Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for developing grounded theory. 2nd Ed.* . Thousand Oaks, CA: SAGE.
- Sutherland, E. (2018). *Digital privacy in Africa: cybersecurity, data protection & surveillance*. SSRN.
- Svabensky, V., Vykopal, J., Cermak, M., & Lastovicka, M. (2018). Enhancing Cybersecurity Skills by Creating Serious Games . *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* , 194-199.
- Symantec Security Center. (2021). *Security Management*. Retrieved from Symantec Security Center: <https://www.broadcom.com/support/security-center>
- TDRA. (2020). *UAE Cybersecurity Strategy* . Retrieved from <http://www.tdra.ae>.

The Washington Post . (2020, 08 06). *Capital One fined \$80 million for 2019 hack of 100 million credit card applications.* Retrieved from https://www.washingtonpost.com/national-security/capital-one-fined-2019-hack/2020/08/06/90c2c836-d7f3-11ea-aff6-220dd3a14741_story.html

The Wharton School of the University of Pennsylvania. (2017, August). *This is what the future of cybersecurity will look like.* Retrieved from World Economic Forum: <https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge>

Valinsky, J. (2020, April 1). *Marriott discloses data breach possibly affecting over 5 million customers.* Retrieved from CNN Business: <https://edition.cnn.com/2020/04/01/business/marriott-hack-trnd/index.html>

Valuch, J., Gabris, T., & Hamulak, O. (2017). Cyber attacks, information attacks, and postmodern warfare. *Baltic Journal of Law and Politics.*

Van Slyke, C., Clary, G., Ellis, S., & Maasberg, M. (2019). *Employer preferences for cybersecurity skills among information systems graduates.* ACM DL Digital Library.

Van Slyke, C., Clary, G., Ellis, S., & Maasberg, M. (2019). Employer Preferences for Cybersecurity Skills among Information Systems Graduates. *In Proceedings of the 2019 on Computers and People research Conference* , 131-134.

Verizon. (2021). *Data Breach Investigations Report.* Verizon. Retrieved from <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

Vidal, J. M., Vidal, J. M., Monge, M. A., & Monterrubio, S. M. (2020). EsPADA: Enhanced Payload Analyzer for malware Detection robust against Adversarial threats. *Future Generation Computer Systems*, 104, 159-173. Retrieved 8 8, 2021, from <https://sciencedirect.com/science/article/pii/S0167739X19310350>

Vigano, E., Loi, M., Yaghmaei, E., Christen, M., & Gordjin, B. (2020). *Cybersecurity of critical infrastructure.* Retrieved 8 8, 2021, from <https://zora.uzh.ch/id/eprint/177141>

- Vijayakumaran, C., Muthusenthil, B., & Manickavasagam, B. (2020). A reliable next generation cyber security architecture for industrial internet of things environment. *International Journal of Electrical and Computer Engineering*, 10(1), 387-395. Retrieved 8 8, 2021, from <http://ijece.iaescore.com/index.php/ijece/article/view/18300>
- Villas-Boas, A. (2019, 06 27). *A Florida city was forced to use pen and paper and pay a \$500,000 ransom after hackers took control of its computers*. Retrieved from Business Insider: <https://www.businessinsider.com/lake-city-florida-ransomware-cyberattack-hackers-bitcoin-payment-2019-6?r=US&IR=T>
- Walter, J. (2020, May 2). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes*. Retrieved from IMC Grupo: <https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/>
- Wellington, J. (2015). *Educational Research: Contemporary Issues and Practical Approaches*. Bloonsbury Publishing .

APPENDICES

Appendix 1: Interview Question's Template – Participant Selection for the Study

Page 1 of 1 Interview Questions – Experiment Program

Student Name	
Major /year	
Date	

Interview Questions:

Question 1: Student Enthusiasm: how much interest did the student shows in the experiment program?

Question 2: Education/Student Major: Development. Motivation to continue learning new skills.

- I noticed on your resume that you are studying_____ program. Please describe the program/major? Why did you choose this field of study?

Question 3: Communication Skills: Ability to communicate effectively, orally and in writing. Shares ideas, concepts and knowledge with others. Listens to, understands and acts constructively with feedback. Possesses effective presentation skills.

- Tell me about a recent successful experience in making a speech or presentation? How did you prepare? How was the speech or presentation received?
- Can you describe a time when you had to work with a remote student or co-worker? How did you stay in touch? What difficulties did you experience?

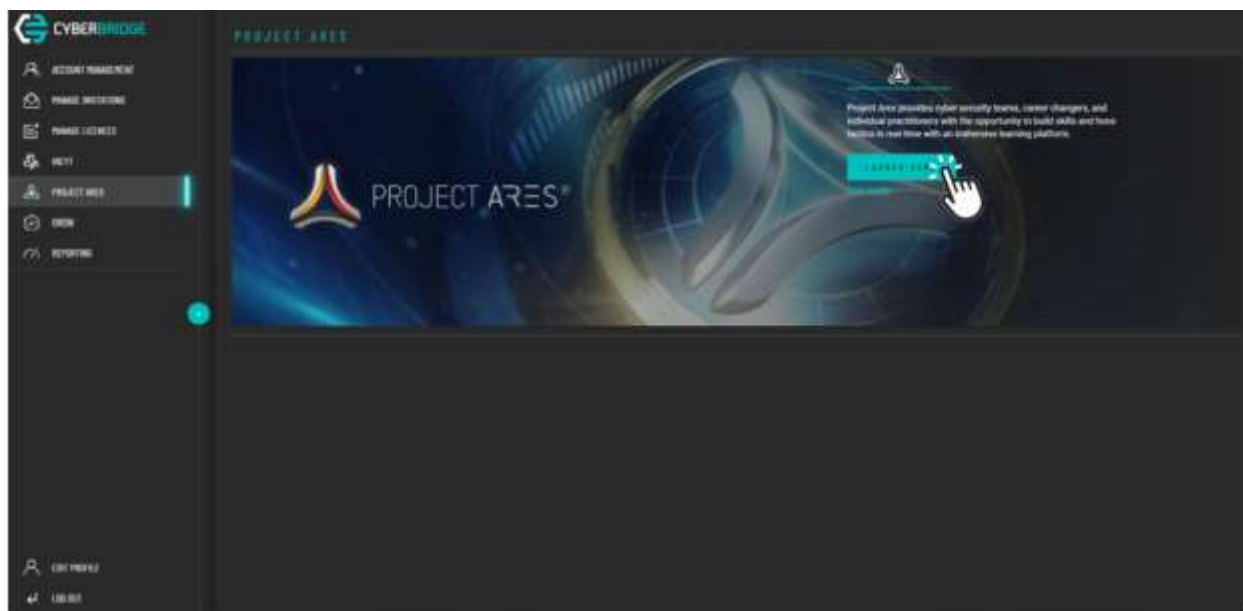
Question 4: Interpersonal Skills: Interfaces well with people at all organizational levels. Has a positive, confident, can-do attitude, which encourages others.

- Give an example of how you've worked on a team.
- What do you do if you disagree with your boss (or a professor)?




Question 5: Technical Knowledge and Skills: Assessing thoroughly the technical knowledge and skills of the undergraduate students.

- Kindly explain the OSI Layer? Difference between TCP/UDP?
- What is digital forensics?
- What are the technical tools you have proficiency in?
- What technical projects have you worked on?
- What was your final year project?

Appendix 2: Cyber Range – Circadence – Project Ares





 <h2>Gamification</h2> <p>Cyber range-based, gamified learning platform Project Ares® prepares students to tackle real-world threats.</p> <ul style="list-style-type: none"> • Project Ares has a series of mini-games, battle rooms, and missions that help engage students in task completion—all while learning new techniques and strategies for defeating modern-day attacks. • By combining interactivity and machine learning with the motivation that gamification provides, students enjoy learning and have a record of progress and growth. 	 <h2>Scale</h2> <p>Compose student teams of any size with access to learning exercises 24x7.</p> <ul style="list-style-type: none"> • On-demand learning for individual skill-building up to full-scale red team and blue team missions. • Cybersecurity students can collaborate and learn from multiple simultaneous locations, from anywhere they have an internet connection. • Your student's group can increase the size and fidelity of their respective environments without a significant increase in cost. 	 <h2>Repetition</h2> <p>Cybersecurity students will be better prepared to enter the cyber workforce with a holistic understanding of offense and defense techniques.</p> <ul style="list-style-type: none"> • Apply the principles of active learning through hands-on interaction and repetition, which increases retention rates to 75% (Training Industry Magazine). • The only solution that provides real-time scenarios that are delivered on an HTML5 compliant platform in a web browser. • Students are minutes from a training event that can be repeated over and over for new learning and skill-building opportunities.
---	--	---

Appendix 3: Cyber Range – Battle Rooms 9 and Mission 8 – Scenario Description

Battle Room 9- Forensics



Load Time	5 min
Time Limit	8 hrs
# of Tasks	39
Hints	Yes
Save Session	Yes
Team Based	No

Scenario Overview:

Player will be given a Windows 10 environment that is accessible through SSH or VNC terminals provided within the scenario. They will conduct entry level task using forensic tools to provide the necessary evidence needed to support a case of an intrusion.


How to be Successful:

The learner must demonstrate the ability to conduct data recovery, disc image analysis, and forensic analysis.

What should you know prior:

Learners should be familiar with basics of host discovery, analysis and data archives gathering.

Mission 8- Defend ICS/SCADA System – Operation Ocean View



DEFENSIVE	
Click For Video	
Load Time	14 min
Time Limit	40 hrs
# of Tasks	4
Hints	Yes
Save Session	Yes
Team Based	Yes

Scenario Overview:

There are reports that the local water authority has just been compromised, putting delivery of clean water for the city at risk. Readings from the water treatment plant's SCADA systems are showing that the chlorine level is 10 times the amount deemed safe for consumption. It's possible that someone gained access to the plant's SCADA system from the inside and were able to override all safety functions.

How to be Successful:

The learner will use network and service analysis to find a Programmable Logic Controller (PLC) that is actively being attacked by an adversary. Through service monitoring, network analysis, and firewall management, they will identify and report the adversary to the intelligence community, implement firewall rules to stop the adversary access to the PLC, and monitor the service post firewall configuration to ensure the services remain running.

What should you know prior:

Learners should be familiar with network infrastructure, management & defense, vulnerability assessment and incident response processes.

Appendix 4: Experiment Program – Calendar Breakdown

Experiment Program – June

June						
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1 June 9 Participants on boarding to the experiment program	2 June Meet and Greet	3 June Phase 1: Assessment Phase Interviewing all 9 participants to assess current technical skills	4 June	5 June
6 Phase 2: Training Phase access provided to Cyber Range – Briefing & Exploration	7 Access provided to Cyber Range Battle Room 9 to execute	8 Introduction to Digital Forensics Lecture Continue Participant work on BR 9	9 Continue training on Cyber Range Battle Room 9 to execute	10 Continue training on Cyber Range Battle Room 9 to execute	11	12
13 Continue training on Cyber Range Battle Room 9 to execute	14 Continue training on Cyber Range Battle Room 9 to execute	15 Continue training on Cyber Range Battle Room 9 to execute	16 Continue training on Cyber Range Battle Room 9 to execute	17 Continue training on Cyber Range Battle Room 9 to execute	18	19
20 Continue training on Cyber Range Battle Room 9 to execute	21 Continue training on Cyber Range Battle Room 9 to execute	22 Continue training on Cyber Range Battle Room 9 to execute	23 Participants to provide feedback on their experience with CR – BR9	24 Participants to provide feedback on their experience with CR – BR9	25	26
27 Phase 2: Training Phase access provided to Capture the Flag – Briefing & Exploration	28 Continue training on Capture the Flag Platform	29 Continue training on Capture the Flag Platform	30 Continue training on Capture the Flag Platform			

Experiment Program – July

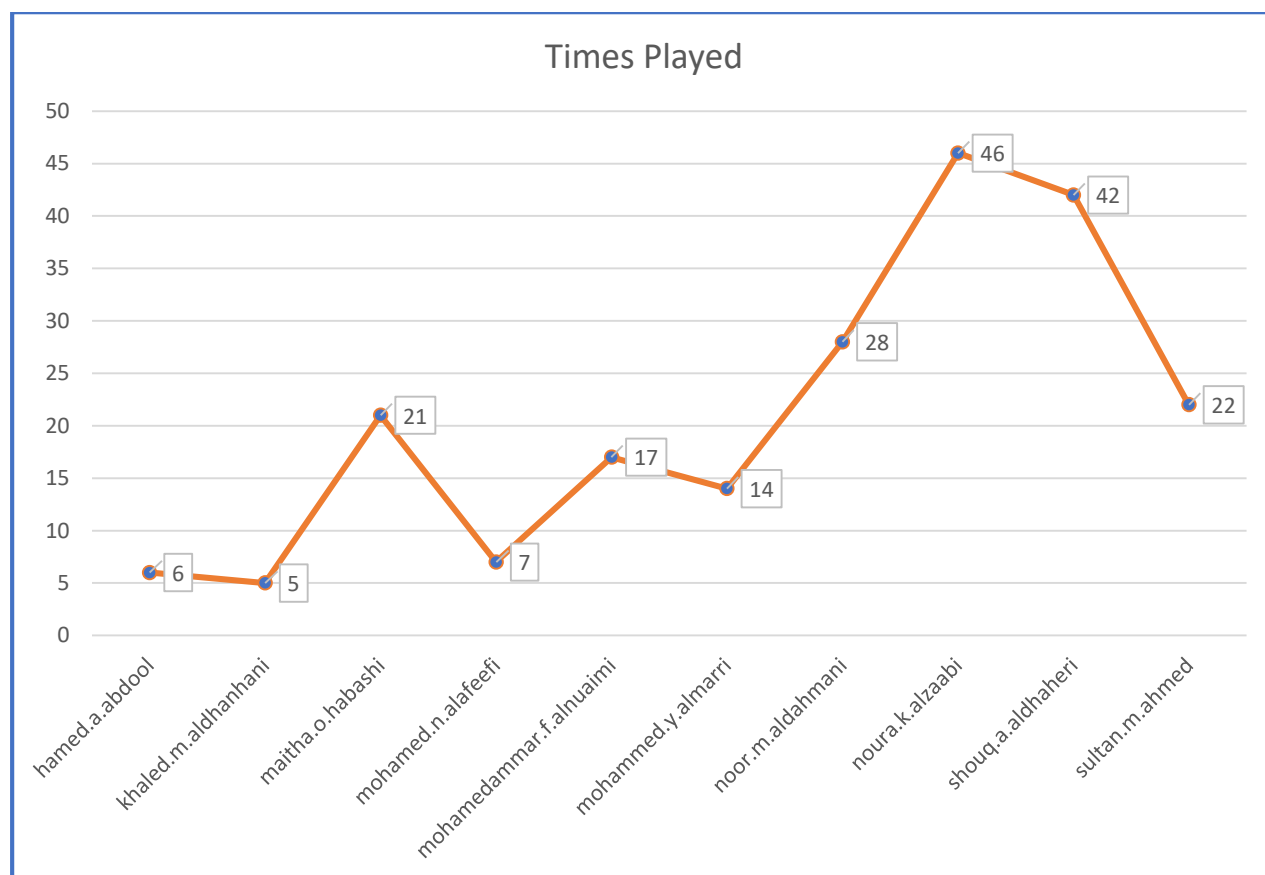
July						
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1 Continue training on Capture the Flag Platform	2	3
4 Continue training on Capture the Flag Platform	5 Continue training on Capture the Flag Platform	6 Continue training on Capture the Flag Platform	7 Participants to provide feedback on their experience with CTF scenarios	8 Participants to provide feedback on their experience with CTF scenarios	9	10
11 Phase 2: Training Access provided to participants for Mission 8	12 Continue training on Cyber Range – Mission 8	13 Continue training on Cyber Range – Mission 8	14 Continue training on Cyber Range – Mission 8	15 Continue training on Cyber Range – Mission 8	16	17
18 Public Holiday / Eid	19 Public Holiday / Eid	20 Public Holiday / Eid	21 Public Holiday / Eid	22 Public Holiday / Eid	23	24
25 Participants to provide feedback on their experience with CR – Mission 8	26 Participants to complete the post-training phase survey questionnaire	27	28	29	30	31

Appendix 5: Cyber Range: BR9 and M8 – Exported Results from Project Ares

BR9 and M8 status (only)

Sum of High Score (Pct)	Column Labels	
Row Labels	BR9E - Forensics	M8E - Operation Ocean View
hamed.a.abdool	100%	100%
shouq.a.aldaheri	100%	100%
noura.k.alzaabi	100%	100%
maitha.o.habashi	100%	100%
sultan.m.ahmed	100%	100%
mohamed.n.alafeefi	100%	100%
mohamedammar.f.alnuaimi	100%	100%
noor.m.aldahmani	97%	100%
khaled.m.alধানহানি	74%	
mohammed.y.almarri	10%	

8	Completed Mission 8
7	Completed Battle Room 9
3	Started but did not complete BR 9
2	Did Not Complete Mission 8



Hints Used in BR9	
Row Labels	Count of Time Spen
BR9E - Forensics	
hamed.a.abdool	
48/157	1
khaled.m.aldhanhani	
90/157	1
maitha.o.habashi	
63/157	1
mohamed.n.alafeefi	
54/157	1
mohamedammar.f.alnuaimi	
0/156	1
mohammed.y.almarri	
12/156	1
noor.m.aldahmani	
128/156	1
noura.k.alzaabi	
120/157	1
shouq.a.alahaheri	
24/157	1
sultan.m.ahmed	
3/156	1

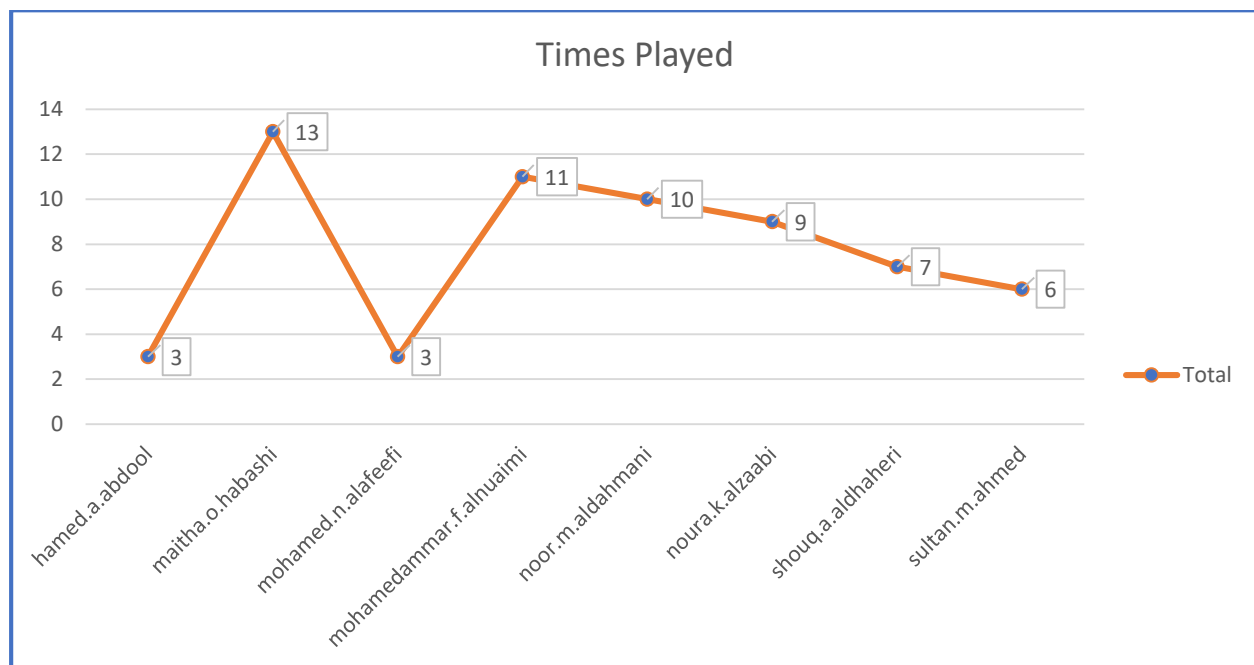
Hints used by participants to complete Cyber Range – Battle Room 9

M8E - Operation Ocean View	
hamed.a.abdool	
6/10	1
maitha.o.habashi	
10/10	1
mohamed.n.alafeefi	
10/10	1
mohamedammar.f.alnuaimi	
0/10	1
noor.m.aldahmani	
0/10	1
noura.k.alzaabi	
6/10	1
shouq.a.alahaheri	
0/10	1
sultan.m.ahmed	
0/10	1

Hints used by participants to complete Cyber Range – Mission 8

Sum of High Score (Pct)	Column Labels
Row Labels	M8E - Operation Ocean View
hamed.a.abdool	100%
maitha.o.habashi	100%
mohamed.n.alafeefi	100%
mohamedammar.f.alnuaimi	100%
noor.m.aldahmani	100%
noura.k.alzaabi	100%
shouq.a.aldhaheri	100%
sultan.m.ahmed	100%

Scores of Participants who completed Cyber Range Mission 8 Scenario



Number of times participants played Cyber Range Mission 8 Scenario

UserName	Activity	Times Pla	Time Spent
sultan.m.ahmed	M8E - Operati	6	03:49:11
mohamedammar.f.alnuaimi	M8E - Operati	11	01:20:23
maitha.o.habashi	M8E - Operati	13	21:23:59
shouq.a.aldhaheri	M8E - Operati	7	02:26:35
noor.m.aldahmani	M8E - Operati	10	01:59:21
noura.k.alzaabi	M8E - Operati	9	02:09:14
hamed.a.abdool	M8E - Operati	3	01:03:53
mohamed.n.alafeefi	M8E - Operati	3	00:55:15

Times Spent by participants playing the Cyber Range Mission 8

UserName	Activity	Times Pla	Time Spent
sultan.m.ahmed	BR9E - Forensi	4	07:18:25
mohamedammar.f.alnu	BR9E - Forensi	6	15:51:31
maitha.o.habashi	BR9E - Forensi	2	9 16:29:37
shouq.a.aldhaheri	BR9E - Forensi	5	14 23:52:39
noor.m.aldahmani	BR9E - Forensi	6	10 08:57:59
mohammed.y.almarri	BR9E - Forensi	11	3 03:44:00
noura.k.alzaabi	BR9E - Forensi	4	4 14:04:59
hamed.a.abdool	BR9E - Forensi	3	5 18:27:14
mohamed.n.alafeefi	BR9E - Forensi	4	15 05:30:53

Times Spent by participants playing the Cyber Range Battle Room 9

Appendix 6: Post-Train Survey Questionnaire – Template

Questions Responses 9

Section 1 of 9

Post Internship Questionnaire

The Internship is an 8 weeks program that consisted of 10 senior/junior year students from various universities across the UAE both male and female who are majored in a computing undergraduate degree with a grade point average of 3.0 and above

Email *

Valid email

This form is collecting emails. [Change settings](#)

Informed Consent

Dear Cyber Security Participant,

This questionnaire is designed to solicit information about the effectiveness of the use of Technical Gamification Simulation Platform (Cyber Range - Circadence) and Capture the Flag Platform (CTF.AE) as methods in order to upscale your technical hands on skills.

For this questionnaire to be helpful and accurate in measuring the effectiveness of the TGSP and the CTF, it is important that you answer each question as honestly as possible.

The information you provide will be used strictly for academic purposes and your identities will be kept anonymous at all time. I will highly appreciate your participation in this questionnaire and your honest and detailed feedback.

Do you wish to participate? *

☐ Yes

☐ No

After section 1 Continue to next section

Section 2 of 9

Declined Participation

You have declined the participation in this questionnaire. Thank you for your time, kindly click "submit form" and close the browser.

Post-Train Assessment Questionnaire:

Introduction:

This experiment program duration is an 8 weeks program that consists of 10 senior/junior year students from various universities both male and female who are majored in a

computing undergraduate degree, specialization of Cybersecurity with a grade point average of 3.0 and above

*** Required**

1. Informed Consent

Dear Cyber Security Participant,

This questionnaire is designed to solicit information about the effectiveness of the use of Technical Gamification Platform (Cyber Range) and Capture the Flag Platform as methods in order to upscale your technical hands-on skills.

For this questionnaire to be helpful and accurate in measuring the effectiveness of the Technical Gamification Platform and the CTF, it is important that you answer each question as honestly as possible.

The information you provide will be used strictly for research purposes and your identities will be kept anonymous at all time. I will highly appreciate your participation in this questionnaire and your honest and detailed feedback.

2. Do you wish to participate? *

Mark only one oval.

Yes - Skip to section 3

No - Skip to section 2 (Declined Participation)

Section 2: Declined Participation

You have declined the participation in this questionnaire. Thank you for your time, kindly click "submit form" and close the browser.

Section 3: Knowledge Questions

In order to become a cyber security professional, one requires Knowledge, Skills and Abilities to perform a specific cyber security role. Knowledge is defined as the information needed to perform a task.

1) I attended 8 weeks long of instructor led training about Introduction to Computer Forensics taught once every week with length of 2hours *

Mark only one oval.

Yes

No

2) The knowledge I gained by attending these lectures are the following: (Select all that applies) *

Check all that apply.

- Investigation, auditing and forensics methods, processes, procedures and standards
- Types of digital forensics data and how to recognize them

- Concepts and practices of processing digital forensic data
- Security event correlation tools
- Different types of hardware, storage, imaging and file system analysis
- Processes for seizing and preserving digital evidence
- Data carving tools and techniques (e.g., Foremost).
- Forensics lab design configuration and support applications (e.g., VMWare, Wireshark)
- Packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Which system files contain relevant information and where to find those system files
- Debugging procedures and tools
- Other:

3) Kindly elaborate what other knowledge have you gained more than the ones mentioned above. * (TEXT ENTERED BY PARTICIPANT)

Section 4: Skills Questions (1) Cyber Range

These questions are related to Technical Gamification Platform used which is the Cyber Range where you were exposed to Battle Room 9 related to Digital Forensics - A Skill is defined as the expertise or talent needed to perform a task

1) I had access for 8 weeks to a Technical Gamification Simulation Platform known as Cyber Range *

Mark only one oval.

Yes

No

2) I had access to Battle Room 9 which is related to a Computer Forensics Challenge for 8 weeks *

Mark only one oval.

Yes

No

3) I was able to execute most / all of the 35+ challenges in Battle Room 9 *

Mark only one oval.

Yes

No

4) I was able to develop the following Technical Hands-On Skills after attending the instructor led course and having access to the Cyber Range platform ((Select all that applies)) *

Check all that apply.

- Programming skills such as C, C++, Java and others.

- System Administration skills for different OS (Windows, UNIX, Linux, Mac OS, Exchange, etc.)
- Preserving evidence integrity according to standard operating procedures
- Analyzing memory dumps to extract information
- Identifying and extracting data of forensic interest in diverse media
- Using forensic tool suites (e.g., EnCase, Sleuthkit, FTK)
- Analyzing anomalous code as malicious or benign
- Interpreting results of debugger to ascertain tactics, techniques, and procedures
- Processing digital evidence, to include protecting sound copies of evidence
- Conducting forensic analyses in multiple operating system environments
- Other:

5) Kindly elaborate what other technical hands-on skills have you developed more than the ones mentioned above from Battle Room 9. * (TEXT ENTERED BY PARTICIPANT)

6) Are you more confident of your technical hands-on skills as you keep executing challenges on Cyber Range after the 8 weeks? *

Mark only one oval.

Yes

No

7) In your honest opinion, do you believe that making Cyber Range platform and CTF part of the Academic Program helps in up scaling a student's technical hands-on skills? In other words, the knowledge gained from the academic degree is reinforced by developing a technical skill using these platforms? Kindly elaborate. * (TEXT ENTERED BY PARTICIPANT)

8) In your honest opinion, if you continued having access to a Cyber Range platform with wide variety of Battle Rooms and Missions will you continue using it to upscale your technical hands-on skills while you are no more an undergraduate student? Kindly elaborate. * (TEXT ENTERED BY PARTICIPANT)

9) In your honest opinion, what additional platform/approach needs to be introduced for undergraduates at their universities/colleagues to have solid technical hands-on skills? Kindly elaborate. * (TEXT ENTERED BY PARTICIPANT)

Section 5: Skills Question (2) Capture the Flag

These questions are related to Capture the Flag platform and the challenges you were able to execute

1) I had access to the Capture the Flag platform where there were several different challenges to execute *

Mark only one oval.

Yes

No

2) Kindly list the challenges that you worked on and successfully executed in the capture the flag * (TEXT ENTERED BY PARTICIPANT)

3) What technical hands-on skills have you gained by working on Capture the Flag platform? Kindly elaborate * (TEXT ENTERED BY PARTICIPANT)

4) Did the Cyber Range experience enhance your technical hands-on skills to successfully carry out Capture the Flag challenges? *

Mark only one oval.

Yes

No

5) Are you more confident of your technical skills as you keep working on challenges on Capture the Flag platform? *

Mark only one oval.

Yes

No

6) In your honest opinion, will you continue to use the Capture the Flag platform to upscale your technical hands-on skills? Kindly elaborate * (TEXT ENTERED BY PARTICIPANT)

Section 6: Abilities Questions

Besides Knowledge and Skills, one develops abilities to perform a given role. An ability is defined as the capabilities needed to perform a task.

1) After attending the instructor led course and having access to both Cyber Range and Capture the Flag as an intern you have the ability to: (Select all that applies) *

Check all that apply.

- Determine how a computer was broken into
- Deal with highly sensitive or confidential data or images
- Decrypt digital data collections
- Conduct forensic analyses in and for both Windows and Unix/Linux environments

- Keep up to date with evolving cyber-crime methods and developments within the digital forensics field
- Present and explain findings and reports when necessary to all interested parties
- Have an analytical mind with the ability to respond quickly to findings
- Provide forensic support to Cyber Security Operations during the investigation of any detected threat or contained incident
- Review detailed incident management reports based on incident investigations
- Use expertise in a corporate setting to protect computers from infiltration
- Other:

2) Any further abilities that you are capable of after attending the Internship?

Kindly elaborate * (TEXT ENTERED BY PARTICIPANT)

Post Internship Proficiency Level

Level 1 - Being Developed (BD): Demonstrates minimal use of this competency. Has limited knowledge of this subject matter area and needs frequent assistance and close supervision for direction. Currently developing skill or competency.

Level 2 - Basic (B): Demonstrates limited use of this competency. Has basic familiarity of subject matter area, and needs additional training to apply with assistance or without frequent supervision.

Level 3 - Intermediate (I): Demonstrates a working or functional proficiency level sufficient to apply the competency effectively without assistance and with minimal supervision. Has working/functional knowledge of the subject matter area.

Level 4 - Advanced (A): Demonstrates in-depth proficiency level sufficient to assist, consult with or lead others in the application of this competency. Has in-depth knowledge in the subject matter area.

Level 5 - Expert (E): Demonstrates broad, in-depth proficiency to be recognized as an authority or master performer in the applications of this competency. Has recognized authority/expert in subject matter area.

3) How do you currently rate your proficiency level post attending the internship in regards to Computer Forensics? (Refer to Proficiency Level defined above) * Mark only one oval.

- 1
- 2
- 3
- 4
- 5

4) What was the reason you picked the proficiency level as mentioned above?

Kindly elaborate * (TEXT ENTERED BY PARTICIPANT)

5) In your honest opinion, what are the most important elements from the list above that helped upscale your technical hands-on skills and expanded your horizon and understanding about Cyber Security that you would want to be included even in your academic year at university/college? Kindly elaborate.

Questionnaire Submission

I sincerely thank you for your honest feedback and the time you have invested in completing this questionnaire. You can complete this questionnaire by clicking on the submit button.

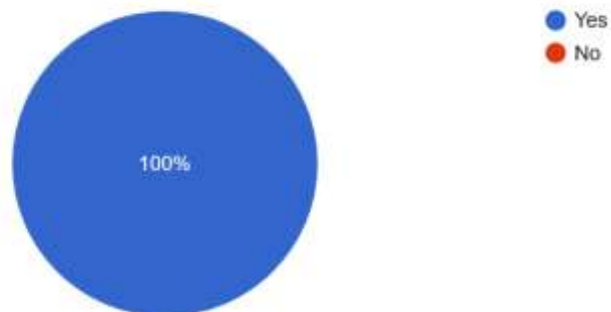
Kind Regards,
Fatma Bazargan

Appendix 7: Post-Train Survey Questionnaire – Participants Responses



Do you wish to participate?

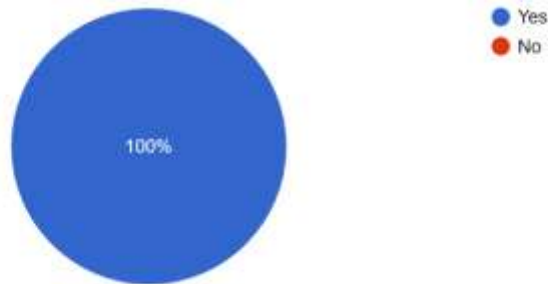
9 responses



Informed Consent of all Participants to take part in the questionnaire.

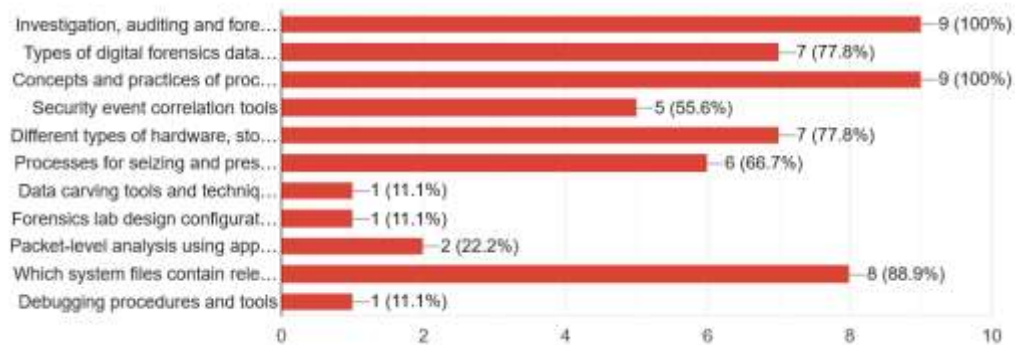
1) I attended an 8 weeks long of instructor led training about Introduction to Computer Forensics by Michael Kaplan - taught once every week with length of 2hours

9 responses



2) The knowledge I gained by attending these lectures are the following: (Select all that applies)

9 responses



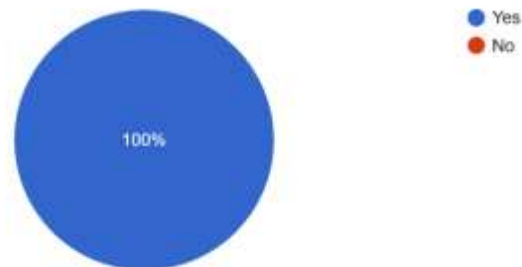
2) I had access for 8 weeks to a Technical Gamification Simulation Platform known as Cyber Range by Circadence

9 responses



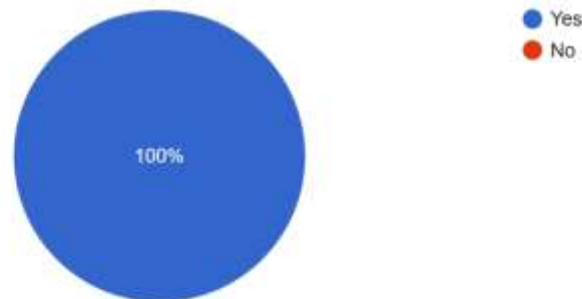
3) I had access to Battle Room 9 which is related to a Computer Forensics Challenge for 8 weeks

9 responses



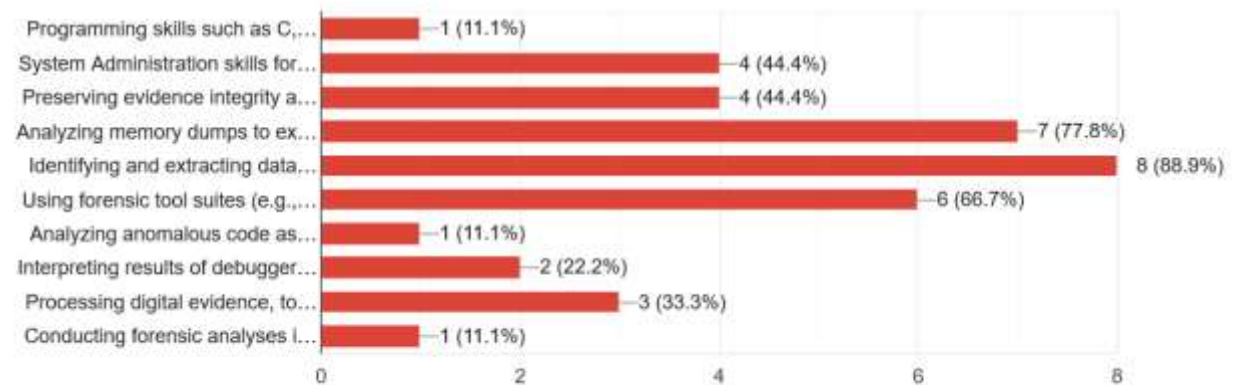
4) I was able to execute most / all of the 35+ challenges in Battle Room 9

9 responses



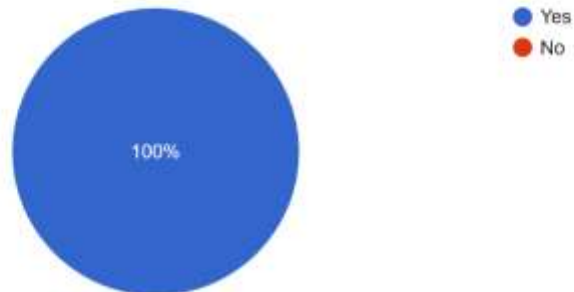
5) I was able to develop the following Technical Hands-On Skills after attending the instructor led course and having access to the Cyber Range platform ((Select all that applies))

9 responses



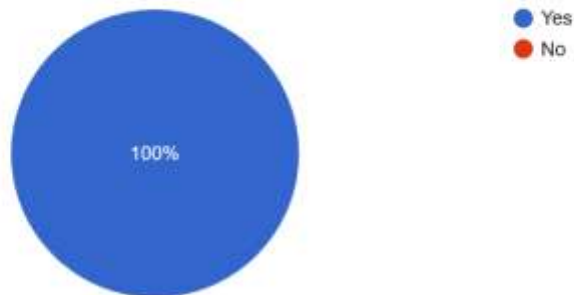
10) Are you more confident of your technical hands on skills as you keep executing challenges on Cyber Range after the 8 weeks?

9 responses



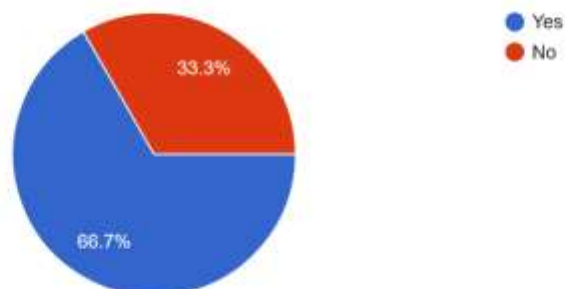
1) I had access to the Capture the Flag platform where there were several different challenges to execute

9 responses



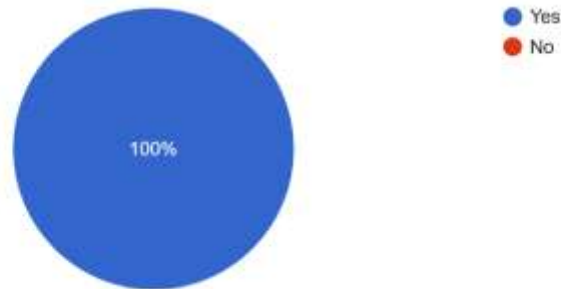
4) Did the Cyber Range experience enhance your technical hands on skills to successfully carry out Capture the Flag challenges?

9 responses



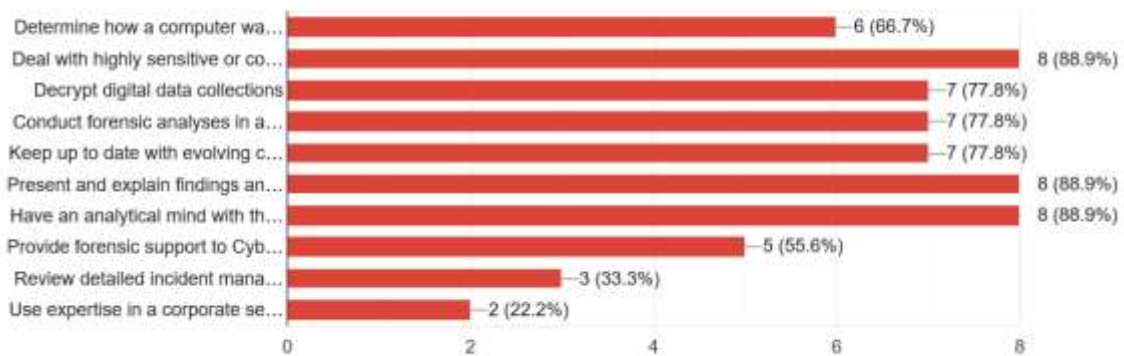
5) Are you more confident of your technical skills as you keep working on challenges on Capture the Flag platform?

9 responses



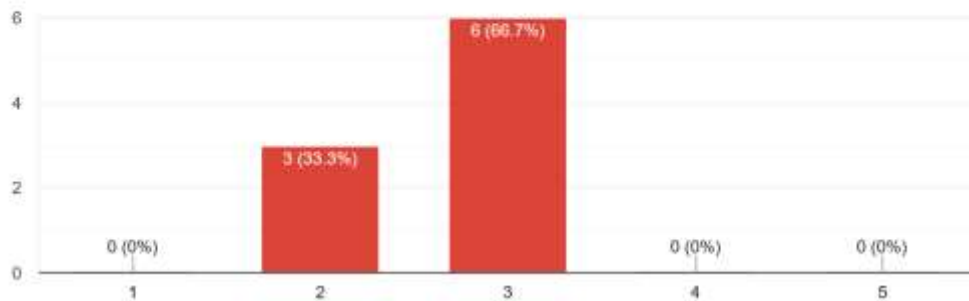
1) After attending the Instructor led course and having access to both Cyber Range and Capture the Flag as an intern you have the ability to: (Select all that applies)

9 responses



How do you currently rate your proficiency level post attending the internship in regards to Computer Forensics? (Refer to Proficiency Level defined above)

9 responses



Proficiency Levels:

Level 1 - Being Developed (BD): Demonstrates minimal use of this competency. Has limited knowledge of this subject matter area and needs frequent assistance and close supervision for direction. Currently developing skill or competency.

Level 2 - Basic (B): Demonstrates limited use of this competency. Has basic familiarity of subject matter area, and needs additional training to apply with assistance or without frequent supervision.

Level 3 - Intermediate (I): Demonstrates a working or functional proficiency level sufficient to apply the competency effectively without assistance and with minimal supervision. Has working/functional knowledge of the subject matter area.

Level 4 - Advanced (A): Demonstrates in-depth proficiency level sufficient to assist, consult with or lead others in the application of this competency. Has in-depth knowledge in the subject matter area.

Level 5 - Expert (E): Demonstrates broad, in-depth proficiency to be recognized as an authority or master performer in the applications of this competency. Has recognized authority/expert in subject matter area.

Screenshots of participants responses to some open-ended questions in the questionnaire.

6) Kindly elaborate what other technical hands on skills have you developed more than the ones mentioned above from Battle Room 9.

9 responses

Navigating and perusing system hives via Registry Explorer.
Finding deleted files and their relevant information.
Obtain important file information, such as modification and access dates.
Extracting important communications (such as email and web browser history) from a drive.

I was able to learn how to use different programs like autopsy for example and obtain data on the client's laptop

- Became familiar with the tool ophcrack, used to crack windows LM and NTLM hashes.
- Navigating the Windows NTFS filesystem and the registry structure to recover evidence.
- Understand Artifacts of execution and where to locate them (shimcache, amcache, prefetch, etc.)

Analyzing data in different parts of a device, using registry explorer to analyze system hives.

i used tools i never did before.
how and where to look for certain type of information

hashes type, attention to details, forensic tools advantages and how they work, recognizing different type

6) Kindly elaborate what other technical hands on skills have you developed more than the ones mentioned above from Battle Room 9.

9 responses

i used tools i never did before.
how and where to look for certain type of information

hashes type, attention to details, forensic tools advantages and how they work, recognizing different type of files like deleted files and root files, cracking password using a forensic tool.

We have used Autopsy.

- I learned how to use Autopsy (A collection of tools grouped into a GUI app) an open source and a very powerful and useful tools in forensics.
- I learned how to analyze an email client, recover messages sent, attachments - (Autopsy)
- I learned how to use Autopsy to recover browsing history (even the deleted ones) - (Autopsy).
- I learned how to browse through registry using various tools such as Registry explorer, such tools makes it easier to understand data within the registry and track changes made on an windows based operating system such as installed applications, removed applications, user-registration info and operating system installation date.

Learned how to use different tools such as Autopsy and Registry explorer

11) In your honest opinion, do you believe that making Cyber Range platform and CTF part of the Academic Program helps in up scaling a student's technical hands on skills? In other words the knowledge gained from the academic degree is reinforced by developing a technical skill using these platform? Kindly elaborate.

9 responses

I believe that the Cyber Range platform and CTF are helpful in 'scaling a student's technical hands-on skills'.
This is because giving a student an outlet for them to actualize their theoretical knowledge in a practical environment allows them to gain an understanding of what works in practice and what is only good in theory.
Learning how to perform many of the techniques required in the Cyber Range and CTF will also be helpful in building the students' technical skills repertoire.

yes i think it helps in scaling up a student's technical skills, because you are exposed to different things and when you get your self familiar with different tools it is easy to master them in the future

Yes I think that they help greatly. Technical hands on exercises like the mentioned (specifically, the CTFs) helped me immensely as a means to apply what I learned, and improve on what I have gained from university and other sources.

They also act as a means to meet like-minded people within the security scene, so they offer a myriad of benefits.

Yes I believe that the Cyber Range platform did help me improve my technical skills. However because of

11) In your honest opinion, do you believe that making Cyber Range platform and CTF part of the Academic Program helps in up scaling a student's technical hands on skills? In other words the knowledge gained from the academic degree is reinforced by developing a technical skill using these platform? Kindly elaborate.

9 responses

Yes I believe that the Cyber Range platform did help me improve my technical skills. However because of the specific design of BR9, since there is no 'story' or like a specific path we should follow, it seemed a bit disconnected. But overall, I did gain forensics skills, and it was a great companion to the lecture.

yes , because it familiarize the students with the technical skills and tools that they need to use in different types of areas.

Yes as that expose them to the reality of how things works and help them to gain the skill of knowing how to start or approach in solving a security issue. Also, to connect their theoretical academic learnings and technical skills in CTF and BR9 into an experience. Make them learn to pay attention to details and help them analyze and gain knowledge about different types of various tools, hashes, codes, sites.

Yes, I believe the cyber range and CTF has helped us develop our technical skills as not all of are in the same level and come from different educational backgrounds.

Definitely, Academic degree cannot cover every technical aspect but it can give the student a taste of it. These CTFs and Cyber range platforms enforces the student's technical skills by putting them into a test to apply their academic and technical knowledge to solve real world like challenges. As a student who

12) In your honest opinion, if you continued having access to a Cyber Range platform with wide variety of Battle Rooms and Missions will you continue using it to up scale your technical hands on skills while you are no more an undergraduate student? Kindly elaborate.

9 responses

In the provided scenario, I would definitely continue using the Cyber Range [CR].

This is because the CR has been a very useful tool for me to further my learning and understand of the field of digital forensics.

I believe that this extends to other fields of cybersecurity, and so would definitely continue practicing on the CR build further skills and sharpen existing ones in different areas of cybersecurity.

for sure i will, because it is a way where i can improve in technical skills. If i had a source that is going to improve it, then i will for sure be using it

Yes I would. The format of the cyber range is more focused when compared to CTFs and the like, allowing us to become much more familiar with the tools used to reach an objective. (e.g. Battle Room 9 wanted to introduce Forensic Analysis with Autopsy as a main tool, and after doing it I feel much more comfortable with utilizing autopsy)

That and I also enjoy doing technical tasks such as those offered in the cyber range.

I would, as the platform seems very helpful with plenty of resources, hints and guides on how to solve the battle rooms/challenges. The fact that each BR is catered to a specific skill would make it helpful for someone who's aiming to improve a certain area/skill they have.

12) In your honest opinion, if you continued having access to a Cyber Range platform with wide variety of Battle Rooms and Missions will you continue using it to up scale your technical hands on skills while you are no more an undergraduate student? Kindly elaborate.

9 responses

I would, as the platform seems very helpful with plenty of resources, hints and guides on how to solve the battle rooms/challenges. The fact that each BR is catered to a specific skill would make it helpful for someone who's aiming to improve a certain area/skill they have.

yes i will continue using them because i know it will help me develop my skills and teach me more things about the cybersecurity world.

Yes I would continue using them as there are many various types of battle rooms and missions to explore and to gain skills from them to practice and crave many skills into me.

I would still use to enhance my technical skills, there is always space for improvement and we need to know what we lack in to work on it.

Definitely yes, as explained in the previous question. These platforms helps me to identify my weakness and strength. In other words, it helps me on improving my weak points and even strengthen my strong points by discovering other ways to perform a certain task.

yes, I always wanted to practice my theoretical knowledge but I did not know where or how to start, I will definitely continue practicing even after graduating.

2) Kindly list the challenges that you worked on and successfully executed in the capture the flag

9 responses

LOOK
Awesome
Keep It Simple
Trail of 404s

LOOK, keep it simple, keep searching, Trail 404s

A total of 13 challenges:
- 4 in Web: Keep It Simple, Keep Searching, Meme Generator, and Lockdown.
- 4 in Reverse Engineering: Slots, Verification Key, Login, Mixed
- 3 in Forensics: LOOK, Super Password, L0oo091n
- 1 in Cryptography: Random
- 1 in Binary Exploitation/Pwn: Pwn 101

Look, Awesome, Keep It Simple, Keep Searching, Trail of 404s

digital forensics : L00k /// web: keep it simple -keep searching /// OSINT: trial of 404s

2) Kindly list the challenges that you worked on and successfully executed in the capture the flag

9 responses

- 1 in Binary Exploitation/Pwn: Pwn 101

Look, Awesome, Keep It Simple, Keep Searching, Trail of 404s

digital forensics : L00k /// web: keep it simple -keep searching /// OSINT: trial of 404s

Completed 5 challenges in Digital forensic (file analyzing), Cryptography (Morse code), WEB (using cookies, finding information) and OSINT (tracing of an account/person)

Look, Awesome, Trail of 404, and Keep it simple.

L00K, Super Password, L00000091n, Awesome, Kryptonite, Keep it Simple, Keep Searching, Trails of 404s

1. Digital Forensics (L00k)
2. Web (Keep It Simple)
3. Web (Keep Searching)
4. OSINT (Trial of 404s)
5. Cryptography (Awesome)

3) What technical hands on skills have you gained by working on Capture the Flag platform? Kindly elaborate

9 responses

While working on the CTF platform, I gained many skills while attempting some of the challenges. These include knowledge and experience using different (some new) tools to tackle some of the challenges, such as disassemblers for the reverse engineering challenges, and password/hash cracking software for the digital forensics and cryptography challenges.

I developed many technical skills, like being able to inspect a web page, decoding hash keys and also problem solving skills when it came for the trail 404 and using different resources on the internet like way back

Its a long list, but honestly every challenge I've performed helped me learn something new within its category.

Web Challenges:

- Better Utilize Burp Suite
- Analyze POST/GET HTTP requests.
- Utilize Python to speed up manual tasks.
- Better utilize SQLMap to pull off SQL injection attacks.
- Understand the concepts of content security policies (CSP), and how they work as protection against XSS.

3) What technical hands on skills have you gained by working on Capture the Flag platform? Kindly elaborate

9 responses

Forensics:

- Utilizing Binwalk/Foremost as anti-stealth tools for data carving.
- Cracking recovered hashes with John and/or hashcat.
- Simple understanding of the ELF file structure.
- Learning about the logical image format ad1, and parsing it with FTK Imager.
- Utilize Registry Explorer to navigate the registry smoothly.

Reverse Engineering:

- Break down execution into small modules to better understand binaries.
- Utilize Disassemblers (e.g. Binary Ninja) to conduct static analysis.
- Utilize Debuggers (e.g. Ollydbg, gdb) to conduct dynamic analysis.

Cryptography:

- Utilize Python to implement the modular multiplicative inverse to reverse the encryption procedure.

Pwn:

- Performing simple buffer overflows.

Web analysis, looking at the network section and cookies. Cryptography skills, recognizing different hashes and encoding methods, and using tools to decode them. Forensics skills like looking into hidden

3) What technical hands on skills have you gained by working on Capture the Flag platform? Kindly elaborate

9 responses

Web analysis, looking at the network section and cookies. Cryptography skills, recognizing different hashes and encoding methods, and using tools to decode them. Forensics skills like looking into hidden files and structures.

use the decoders.

the usage of proxy tools.

the usage of the open source searching engines.

Analyzing information and content, Types of hashes and encodes like Base64, the importance of web Inspecting (how cookies can be used), patience to take it easily while searching and paying attention to details.

I have been exposed to many different tools and have searched a lot on how to solve different challenges. I learned how to decode hashes using online tools and that there are hidden files. In addition, I learned how to use Wayback and how to change cookie values.

Developing a python script to reverse a hash, Discover hidden files within a ZIP file, enforced my skill in performing dictionary attack using john the ripper, enforced my skill in using web proxies to deliver web-

6) In your honest opinion, will you continue to use the Capture the Flag platform to up scale your technical hands on skills? Kindly elaborate

9 responses

I will continue using the CTF platform to enhance my technical hands-on skills, as the skills necessary to complete the CTF challenges are an integral part of the cybersecurity technical skillset. I will also pursue other CTF platforms to expand my horizons and diversify my approach.

Yes for sure, because i think after i completed some of the challenges, i felt more confident and i want to keep on improving.

Yes for sure. I find CTFs enjoyable and highly useful, and will keep doing them for a long time.

Yes I would, it seems like a good platform to check whether you really have gained a certain skill, and since you get to work on it however way you like, you get to keep exploring different software at your own leisure.

yes because it will help me improve my technical skills and it will keep interested.

Yes as it puts you more into the reality of analyzing and investigating. It have different interesting categorizes. It helps on developing critical thinking and makes you gain more information about tools, vulnerabilities, how the network works and vocabularies/topics.

6) In your honest opinion, will you continue to use the Capture the Flag platform to up scale your technical hands on skills? Kindly elaborate

9 responses

Yes I would, it seems like a good platform to check whether you really have gained a certain skill, and since you get to work on it however way you like, you get to keep exploring different software at your own leisure.

yes because it will help me improve my technical skills and it will keep interested.

Yes as it puts you more into the reality of analyzing and investigating. It have different interesting categorizes. It helps on developing critical thinking and makes you gain more information about tools, vulnerabilities, how the network works and vocabularies/topics.

Yes, I will continue to work on CTF platform; I have benefited a lot, and will benefit a lot. It has diverse challenges that I am not exposed to before.

definitely yes, as explained in previous questions. Capture the flag platforms puts my technical skills into test. It helps me improve my skills according to the difficulty faced in solving challenges on different categories.

Definitely! I am glad that I was exposed to the CTF platform, it made me curious to learn and to find ways to complete all the challenges

2) Any further abilities that you are capable of after attending the Internship? Kindly elaborate

9 responses

Process and handle evidence relating to an investigation.
Obtain hidden or protected files via forensic tools.
Identify potential threats in a computer network or system.
Assess and implement cybersecurity policy through certain platforms (Windows Server).

I think, before this internship started most of the knowledge i had that have to do with forensics and investigation were very little and limited. i feel like i am getting a better understanding and knowledge in both theoretical and technical skills. Since i am in my third year i think i got a very good insight on cyber security in general and when i return to my studies most of the things will be familiar to me and i will have the knowledge already and will build more knowledge on top of what i have

- Reverse Engineer Binaries, for both static and dynamic analysis, with the purpose of understanding its functions and how it executes.

I feel that I'm able to analyze data, recognize different types of data and make conclusions on how to work with them. I'm able to think differently based on the situation given as well.

no

2) Any further abilities that you are capable of after attending the Internship? Kindly elaborate

9 responses

I feel that I'm able to analyze data, recognize different types of data and make conclusions on how to work with them. I'm able to think differently based on the situation given as well.

no

Connecting what I learned in university and what reality of cyber security is, differentiate various fields of cyber security, the ability of managing time and understand the roles of security and networking. The importance of building up connections.

Other than the technical skills that we have worked on, I have learned a lot from the different amazing minds that I have been working with. Everyone is unique and thinks differently. Taking the internship with many students makes you learn a lot, as everyone comes from different backgrounds and different educational levels. We learned how to communicate and create our network.

Active listening, I learned how to stay focused and ask related questions in meetings, lectures about discussed topics.

N/A

2) What was the reason you picked the proficiency level as mentioned above? Kindly elaborate

9 responses

I believe that my current proficiency allows me to perform given tasks without impeding or slowing down an operation, but is not enough to lead a dedicated team or head an operation.

Honestly, before this internship i would have picked 1. because with regards of computer forensics, i havent taken any in depth courses, now when it comes to it, i feel like it went up and i am more motivated to pick a 5 in the future.

After acquiring the theory on digital forensics from the course sessions with Mr. Michael Kaplan, I was able to perform forensic analysis on an image with minimal hint usage and apply what I learned throughout the process.

I'd classify myself somewhere between Basic (2) and Intermediate (3), due to the fact that while I am now familiar with the forensic tools and I am able to extract evidence where needed and present them, I still feel more exposure is necessary to become truly intermediate or reach advanced/expert levels.

Although I gained a lot of knowledge, there is still a lot of skills, knowledge, processes I need to learn to be able to feel confident in my skills. I do trust my instincts in the subject, but I know I need to learn more.

2) What was the reason you picked the proficiency level as mentioned above? Kindly elaborate

9 responses

feel more exposure is necessary to become truly intermediate or reach advanced/expert levels.

Although I gained a lot of knowledge, there is still a lot of skills, knowledge, processes I need to learn to be able to feel confident in my skills. I do trust my instincts in the subject, but I know I need to learn more.

because i think i need to improve my skills in the digital forensics field and i need to practice more on it.

As I do have the knowledge of forensics and the a basic functional knowledge, I need more practice and development in technical skills. The internship have provided basic skills and information that will relate to most of the fields and companies.

I feel like I have learned a lot, but still not good at it. I would say decent skills.

I picked intermediate because I have in-depth theoretical understanding of cyber security attacks and I am able to demonstrate them although some do require further practice to master them, then I would consider myself in an advance stage.

digital forensics is a new topic for me, I still need a lot of practice and training to be more confident.

2) In your honest opinion, what are the most important elements from the list above that helped up scale your technical hands on skills and expanded your horizon and understanding about Cyber Security that you would want to be included even in your academic year at university/college? Kindly elaborate.

9 responses

Regarding technical hands-on skills, I believe that access to certain platforms such as the Cyber Range and the CTF challenges were extremely helpful.
If I had access to these platforms during my first or second year of university, I believe I would have been much further along the path of developing my technical hands-on skills.

in terms of the technical skills that helped me, CTF and BR9 and the introduction to computer forensics.

All above points were greatly helpful in their own way, but to pick a few I would say the following points were the most crucial:

- The mentorship from Fatma Bazargan:
- Talks with the various cyber security leaders.

The many great advices and experiences we received from both our mentor Fatma and through the talks were things that I genuinely wish that I received way earlier in university.

Mentorship by a Cyber Business Lead, having someone to guide us in all areas, technical and Cyber Security wise was great. If students had guidance in their university, and were encouraged to improve their technical skills in such early stages they would be much prepared.

2) In your honest opinion, what are the most important elements from the list above that helped up scale your technical hands on skills and expanded your horizon and understanding about Cyber Security that you would want to be included even in your academic year at university/college? Kindly elaborate.

9 responses

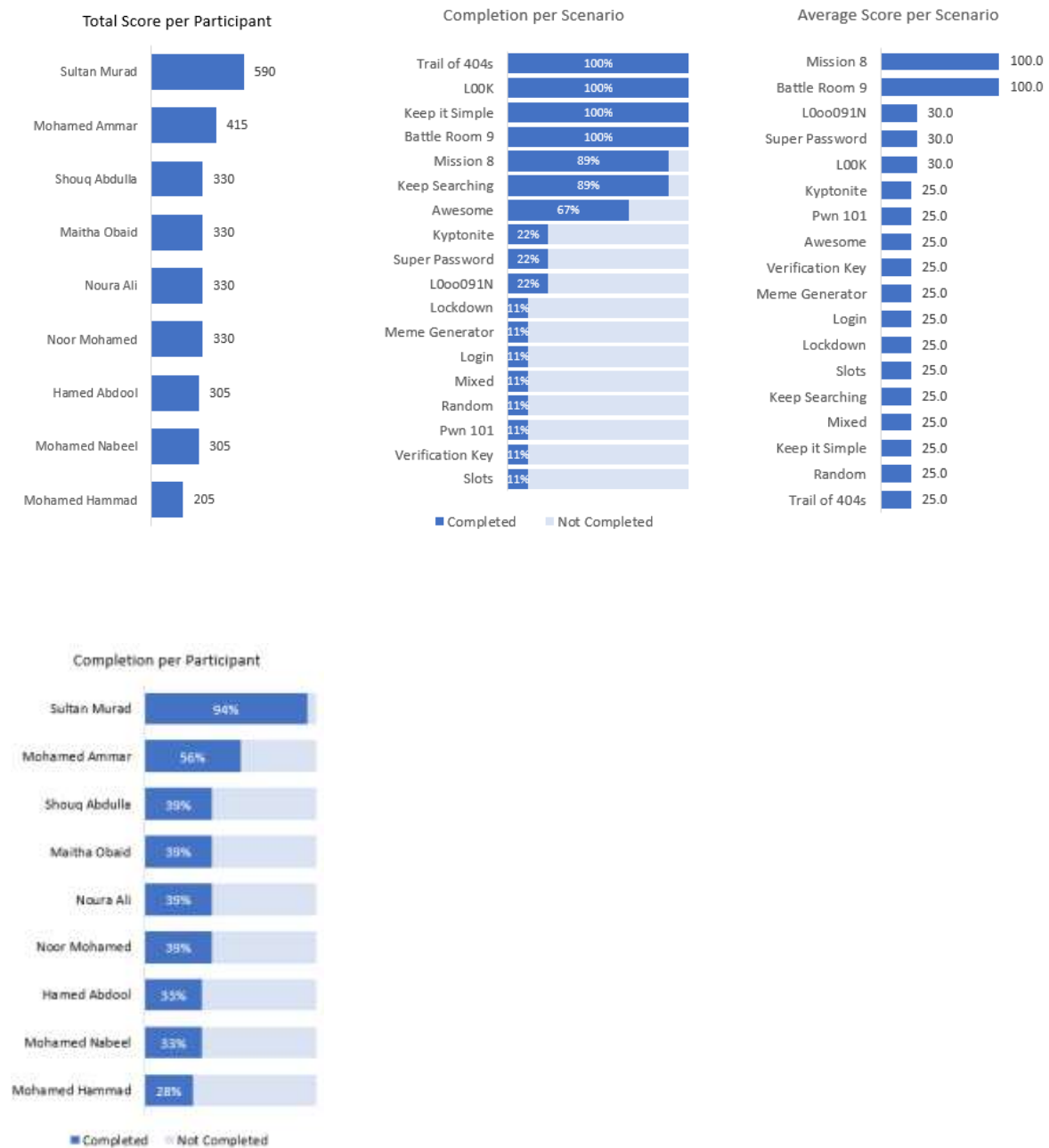
Access to Technical Gamification Simulation Platform - battle room 9, because it helps us by providing hints to understand the way to finish the tasks and you can challenge yourself by finishing the tasks without the hints at the same time.

Battle room 9 and Capture The Flag for technical skills challenges and developing, Cyber Security Leaders/Experts Talks to understand many types of fields and gain good advices for future career, site/tour visits that will help on knowing the reality of working environment.

Battle Room 9 and Capture the Flag Platform. In addition, the expert talks and site visits, I think it would be very helpful to expose students as soon as possible.

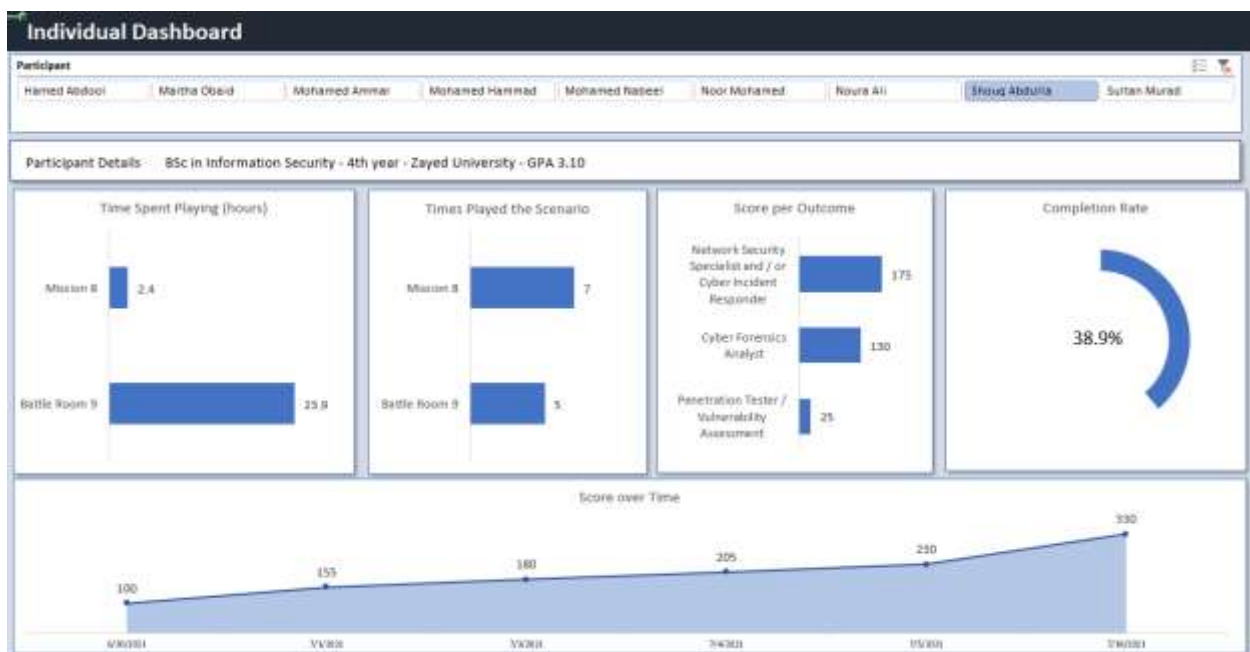
every single point that has been listed. From meeting industry experts and leaders to summarizing our work, I got exposed to up-to-date cyber security concerns and threats. practiced and improved my theoretical knowledge and assisted me in putting the most of my effort to learn more about cyber security on my own. Summarizing our work helped to remind me of what I have been exposed to, the things that interest me and decide the next steps to take. Universities should expose students to the market so the students can pick the right path and dedicate themselves to a field they are passionate in and additionally have a basic knowledge of all other fields within cyber security.

Appendix 8: Skills Performance Dashboard Scores of Participants

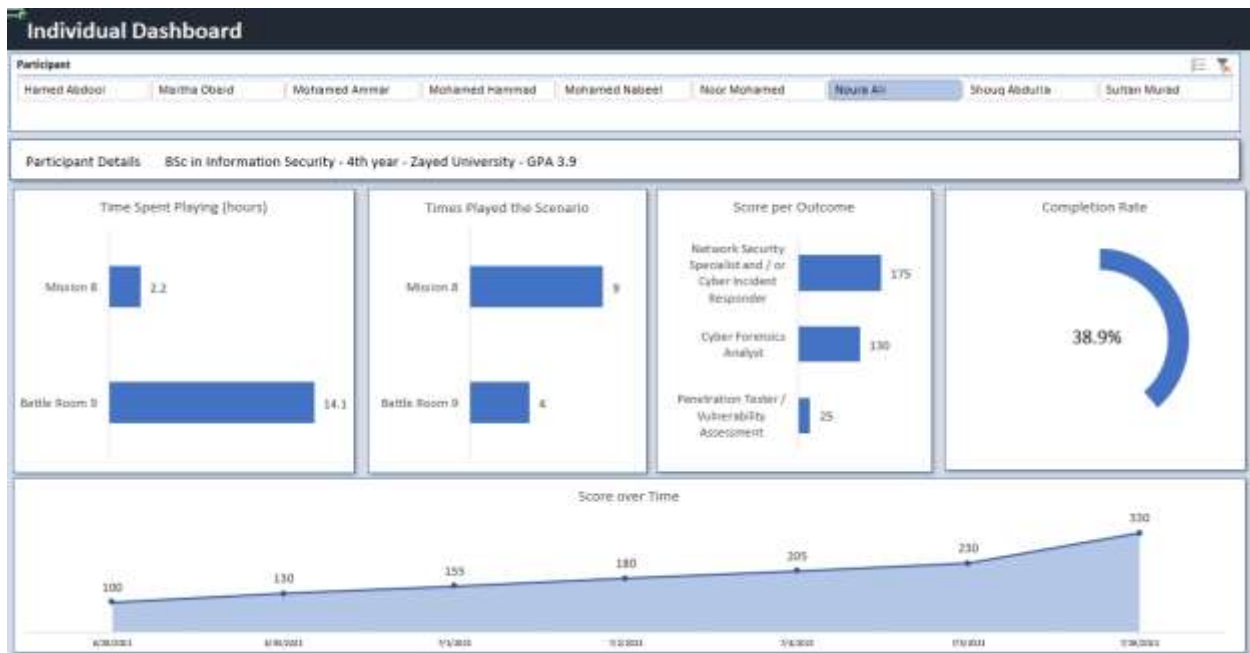




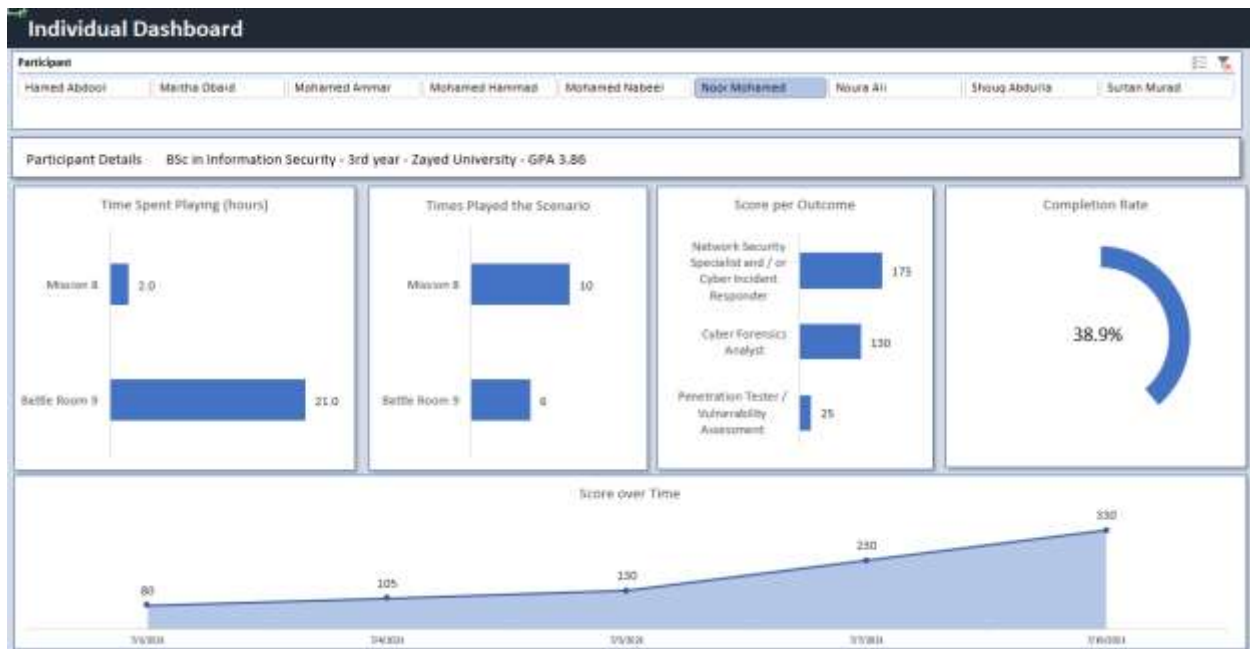
Participant 1 Results



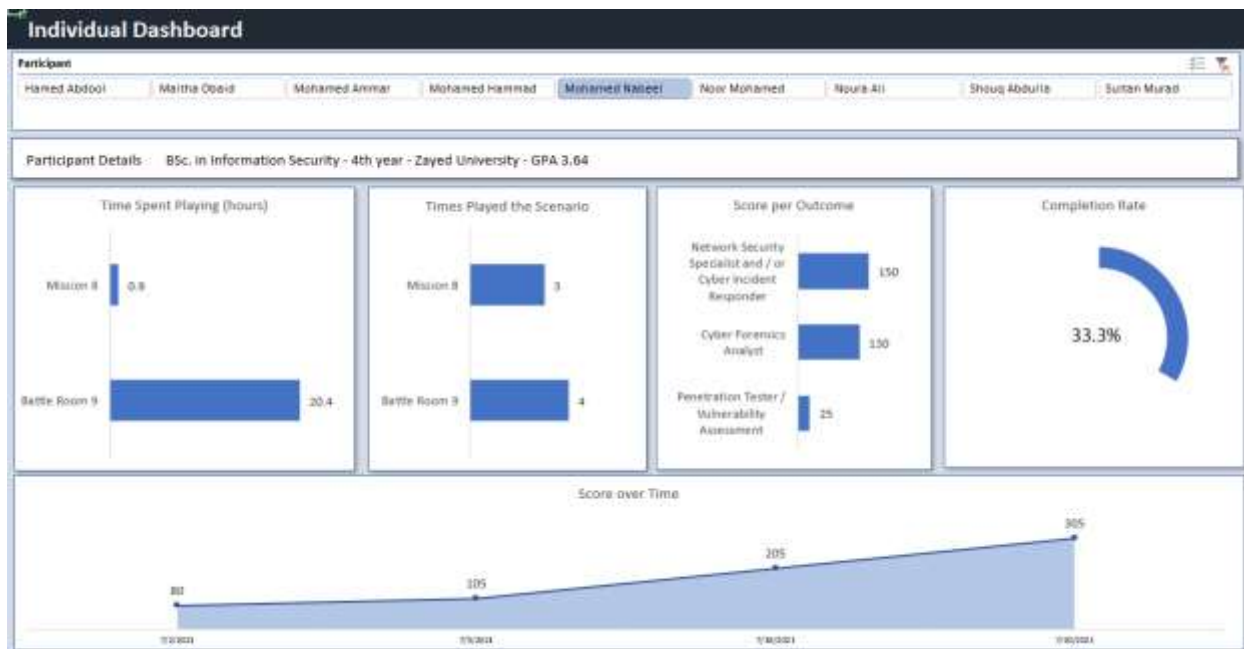
Participant 2 Results



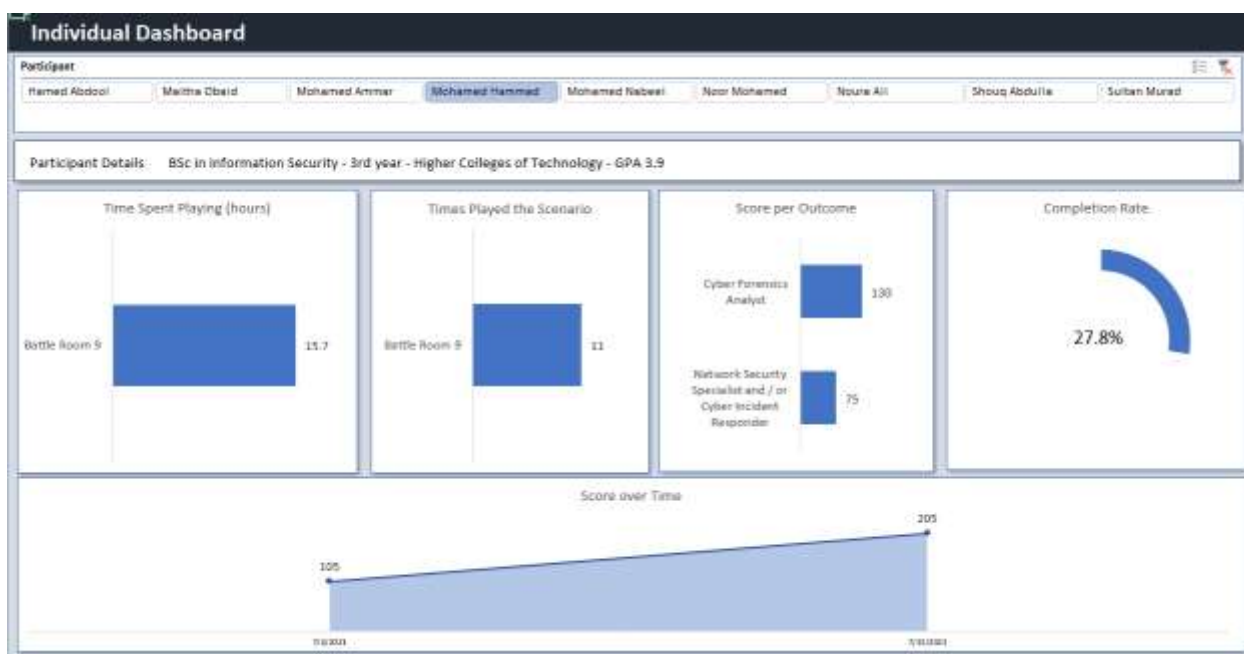
Participant 3 Results



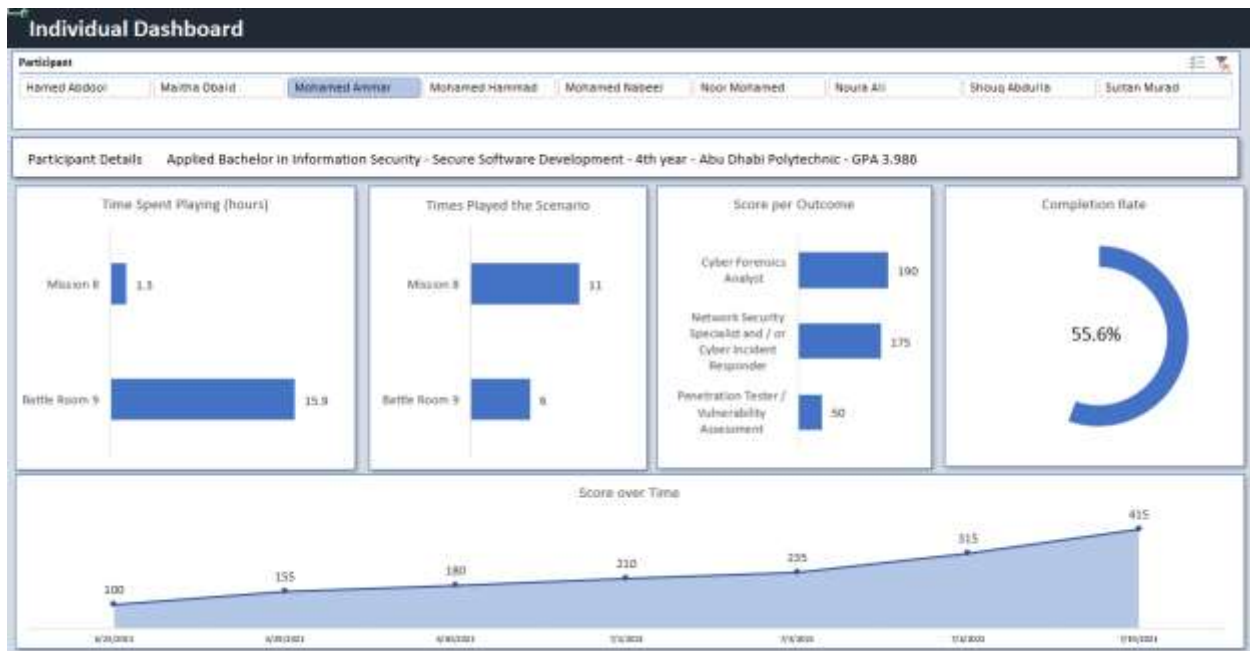
Participant 4 Results



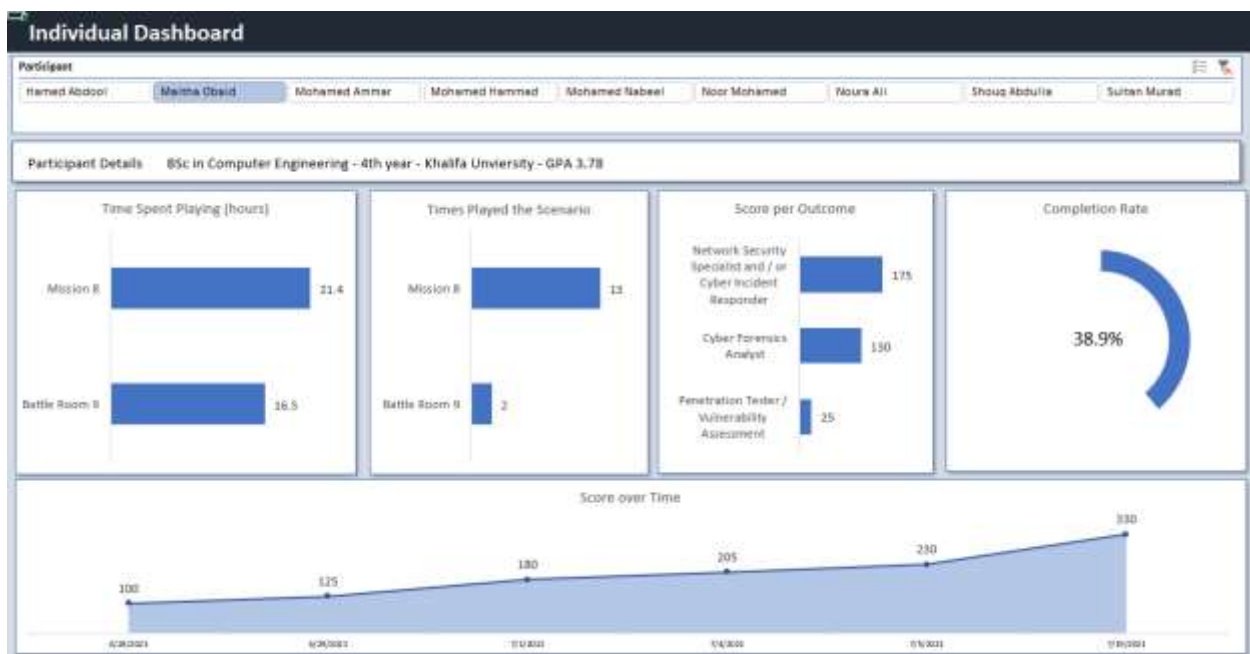
Participant 5 Results



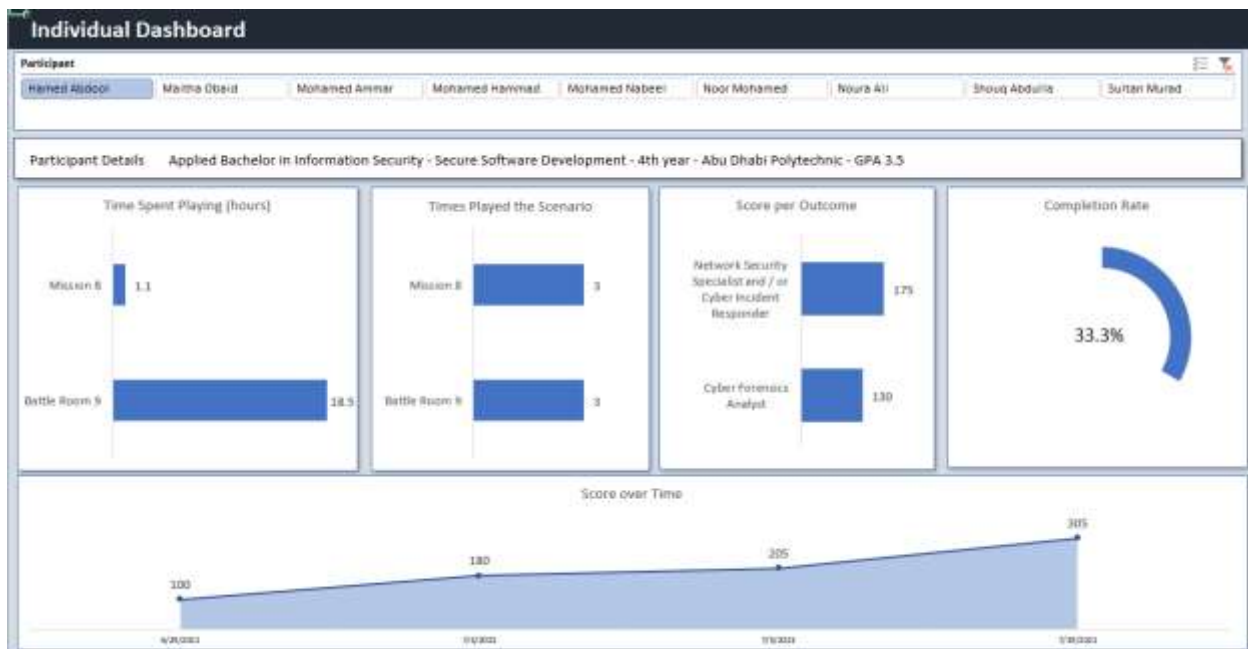
Participant 6 Results



Participant 7 Results



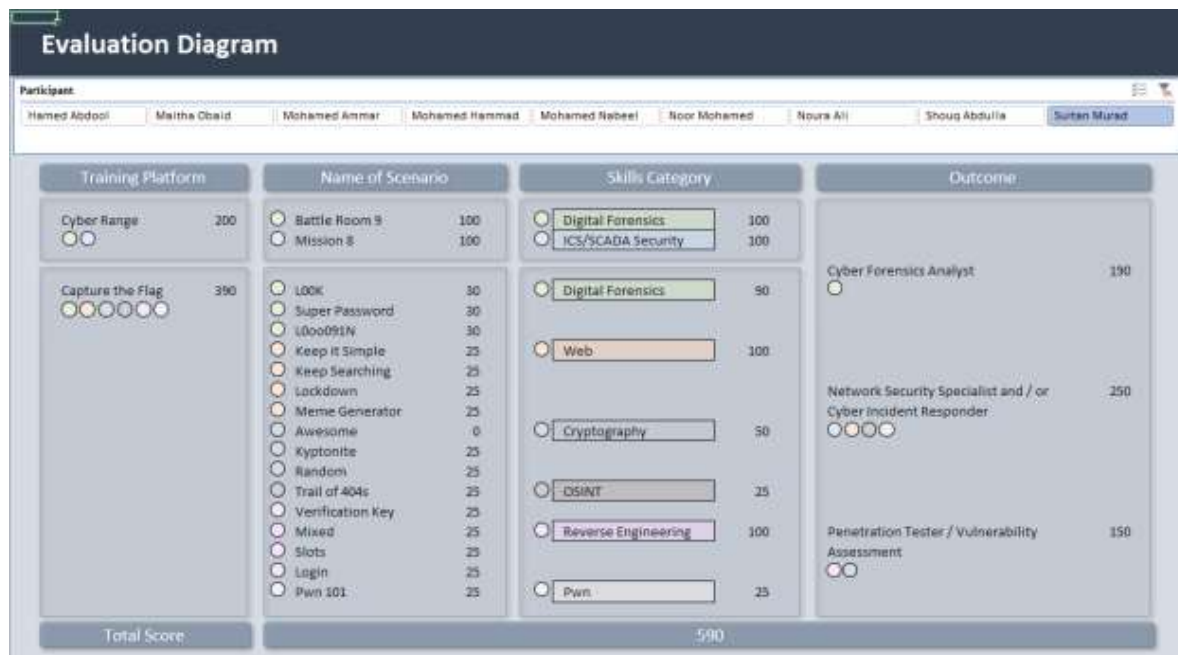
Participant 8 Results



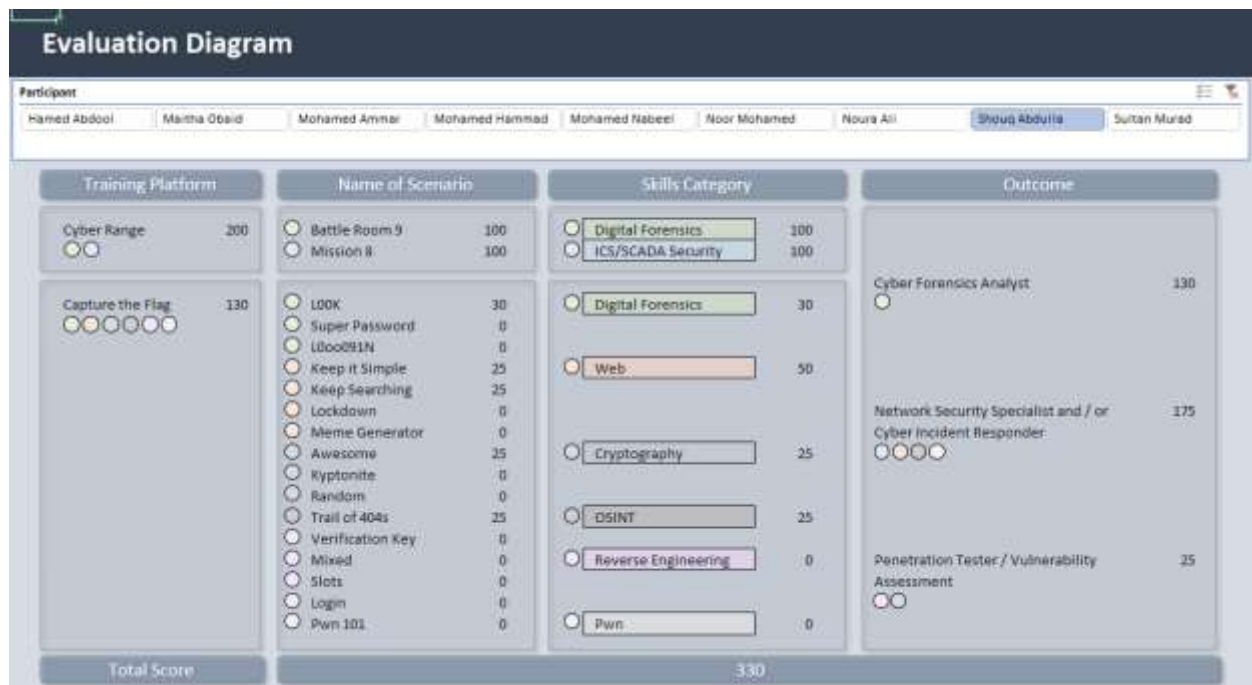
Participant 9 Results

Above Screenshots are the Scores from completing the scenarios and challenges on both the training platforms.

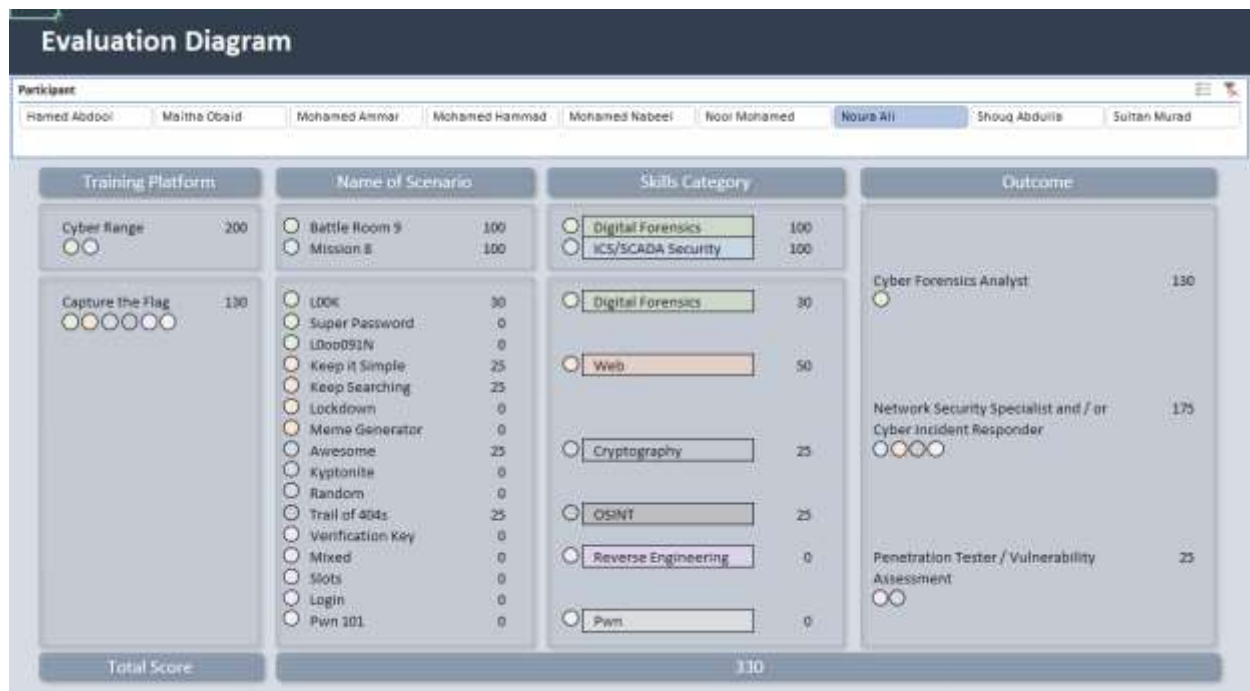
Below screenshots is to show what skills each participant has gained after completing the scenarios and challenges from those two training platforms. Also, the below screenshots provide insights to the viewer which participant they should choose to interview after knowing what technical skillset every participant or practitioner has.



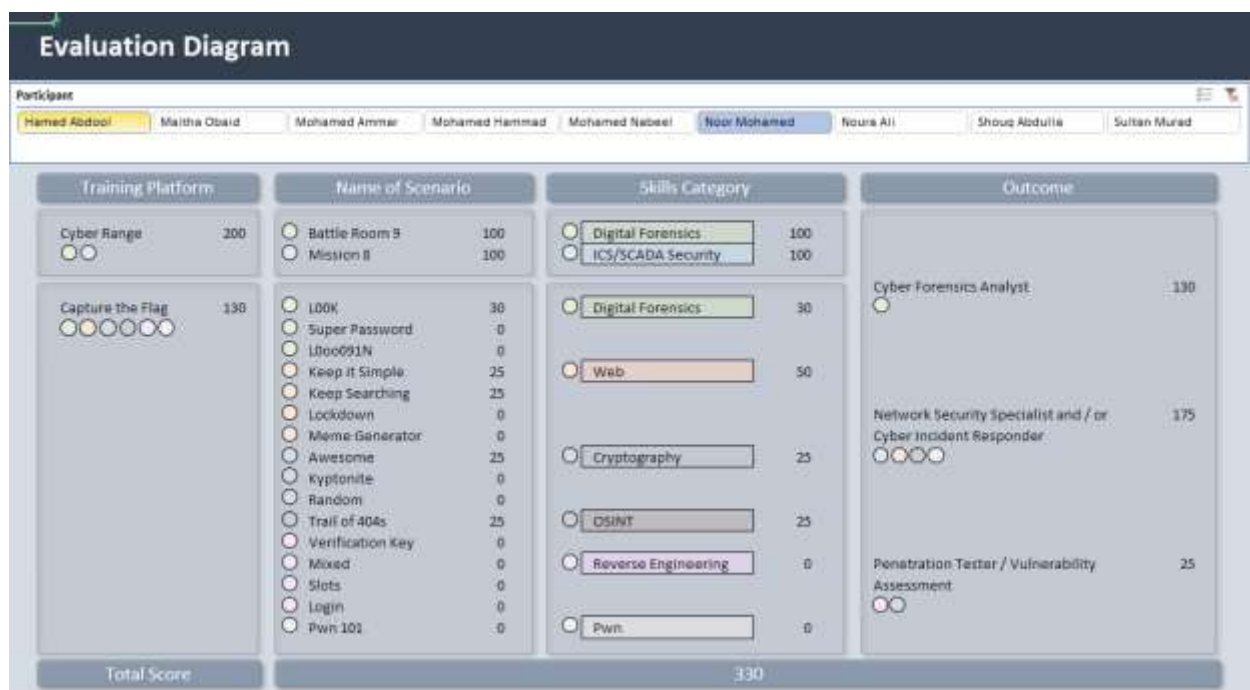
Participant 1 technical hands-on skills



Participant 2 technical hands-on skills



Participant 3 technical hands-on skills



Participant 4 technical hands-on skills



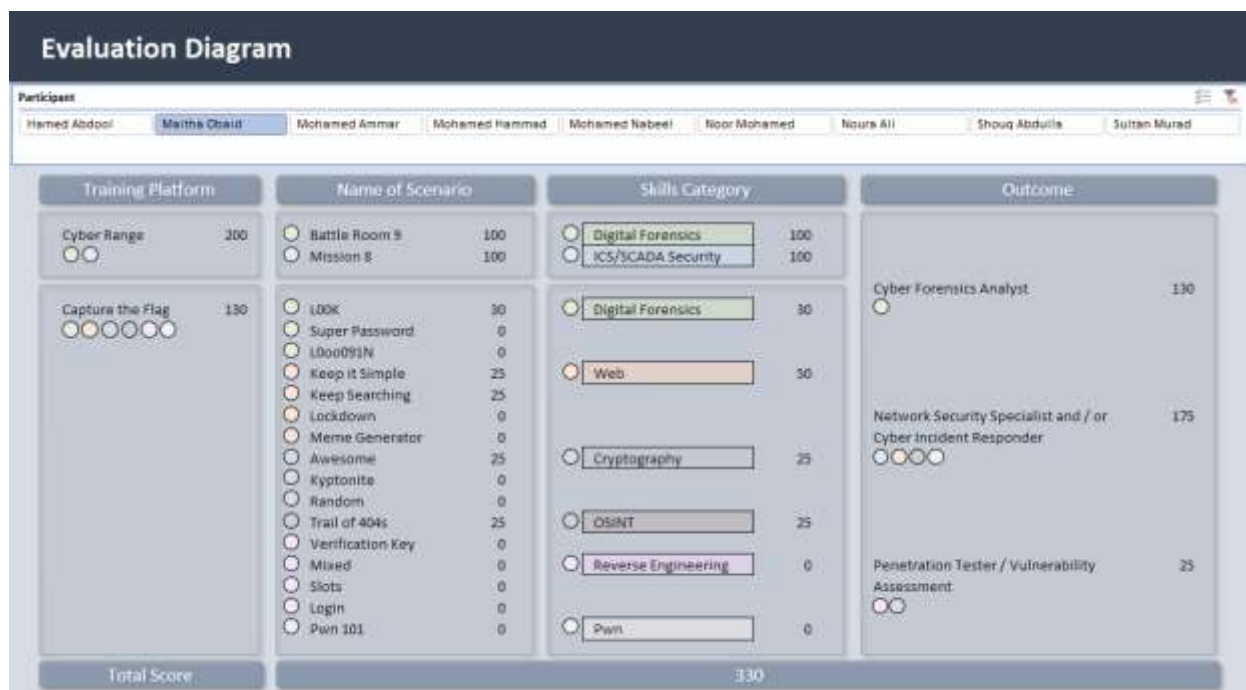
Participant 5 technical hands-on skills



Participant 6 technical hands-on skills



Participant 7 technical hands-on skills



Participant 8 technical hands-on skills



Participant 9 technical hands-on skills

Appendix 9: MAXQDA – Survey Questionnaire – Qualitative Data Analysis

