Cybersecurity Training Platforms: A Comprehensive Review

[1]Arjun Devadas, [1]Alvin Shiju, [2]Sakila K S, [3]Meesam Raza

[1]Undergraduare Student, Department of Cyber Security, British University College, Ajman, United Arab Emirates.

[2*]Lecturer, Department of Cyber Security, British University College, Ajman, United Arab Emirates.

[3]Lecturer, Department of Information Technology, British University College, Ajman, United Arab Emirates.

[*]CS-Faculty@britishcollege.ae

Abstract *:* Cybersecurity is a basic part of present-day business tasks, with the rising recurrence and refinement of digital dangers. To address this test, various internet-based stages have arisen, offering network safety instructional classes, certificates, and viable activities for people and associations trying to upgrade their security abilities. This article presents a complete survey of such stages, looking at their highlights, course contributions, certificate choices, useful activities, and viability in expertise improvement. The audit considers factors like course satisfied quality, educator ability, involved learning potential open doors, industry acknowledgment, and client criticism to give experiences into the qualities and shortcomings of every stage. By integrating this data, people and associations can pursue informed choices while choosing network safety preparing stages to meet their acquiring targets and ability improvement needs.

Index Terms-Cyber Security, Course contributions, Network safety, Expertise improvement, Tracer FIRE

I. INTRODUCTION

Cybersecurity training activities are fundamental for giving the IT labour force the necessary information and reasonable abilities for taking care of the online protection dangers that undeniably compromise all [1]. Different sorts of frameworks connected with online protection preparing, like Capture The Flag (CTF) stages, have been accessible for just about multi decade, however they just incorporate basic errands and don't give virtual organization conditions to students [2]. Nevertheless, a few stages that help sensible undeniable online protection preparing practices have been created and delivered as open source lately (Cyber Range Organisation and Design (CROND), 2022b; Masaryk University, 2022) [3].

Many of these cyberattacks are credited to weaknesses related with human entertainers inside the association. For instance, the episode at Volkswagen came about because of data put away in an unstable document, and the assault on Provincial Pipeline was supposed to be brought about by a re-utilized secret phrase. Assaults on advanced education establishments in the UK are accounted for to happen most frequently through phishing assaults [4]. Harm on account of human activities (or the oversight thereof) can be extreme, with results including loss of efficiency, money related misfortunes, and loss of validity and notoriety [5]. Moreover, results are frequently not promptly apparent. This adversely influences the need to get moving workers partner with network safety [6].

We consider that any network protection preparing stage should cover the three vital parts of preparing: (I) content representation, (ii) environmental management, and (iii) training facilitation [7]. The preparation content is the arrangement of unequivocal or implied assignments that the members should tackle, along with the portrayal of the organization climate the members should connect to address those undertakings. For the preparation to occur, that network climate — which is made of virtual or actual hosts — likewise should be made and made do[8]. The term digital reach is frequently utilized for this climate, however in this paper we on the other hand utilize the term sandbox for clearness purposes. Moreover, different preparation help elements can be utilized during the preparation, for example, allocating undertakings to members through the preparation stage or following their advancement [9].

DOI: 10.55041/IJSREM36016

II. METHODOLOGY

2.1 SUBJECTS:

Subjects comprised of a sum of 26 people who assented to information assortment during two separate Tracer FIRE network protection preparing works out. There were 11 subjects from the principal occasion which happened throughout the spring of 2014 and 15 subjects from the second occasion that happened in the mid-year of 2014 [10].

2.2 PROCEDURES:

The Tracer FIRE practice comprised of a multi-day occasion that consolidated homeroom guidance in the utilization of network protection programming devices, measurable examination methods, and enemy strategies and procedures with a group contest work out [11]. Toward the start of the opposition, there was a declaration concerning the review and those able to agree to information assortment went through the educated assent process. Information assortment with respect to human-machine exchanges happened non-rudely through robotized information logging as subjects partook in the activity. The activity introduced groups a staggered challenge. At a low level, there was a progression of riddles that permitted members to practice their digital measurable examination abilities, as well as the network protection programming instruments. At a more significant level, there was a mind-boggling situation to some degree considering true occasions that elaborate numerous foes with contrasting goals working exclusively and in a joint effort with each other. As members tackled the singular riddles they got focuses that were counted on a scoreboard and opened more riddles. Moreover, by tackling individual riddles, members acquired hints to the general situation that would be useful in addressing resulting puzzles. At the end, each group introduced their understanding of the general situation and a definitive result pivoted upon how intently the group translations compared with the ground reality of the genuine occasions [10].

2.3 TRACER ‘FIRE’ INSTRUMENTATION

Every understudy was furnished with a PC which fundamental digital protection programming devices had been introduced which included EnCaseEnterprise, Wireshark, PDF Dissector and Unpredictability. Workstations additionally offered the essential apparatuses accessible with the Microsoft Windows and Microsoft Office items. Understudies were allowed to download extra programming apparatuses and introduce them on PCs utilized for the activities. An electronic game server gave the premise to members to get to individual difficulties, present their responses and get input showing on the off chance that their responses were right. Furthermore, a news server gave occasional declarations in regard to occasions pertinent to the general situation (e.g., public statement from Hacktivist bunch). A Sandia National Laboratories software tool known as Hyperion was utilized to catch human-machine exchanges [12]. This incorporated the utilization of programming applications (explicitly, setting the console/mouse input concentration to the application), Web gets to, windows occasions, keystrokes, and mouse clicks. The information gathered from Hyperion was joined and synchronized with the game server endlessly logs from of the news server to give a consolidated record enveloping the exercises of every individual member. For every human-machine exchange, the information included:

- Participant UserID
- Timestamp
- xInterval since past exchange (i.e., length)
- Challenge ID, for exchanges including the game server Robert G. Abbott et al. /Procedia Assembling 3 (2015) 5088 - 5094 5091.
- Occasion Type, for exchanges including game server.
- Submission, answer submitted for exchanges including submitting reply to game server.
- Points Granted, for exchanges including submitting replies to the game server.
- Software Tool, for exchange including programming devices.
- Class of Event (Windows, Game Server, or News Server)
- Article ID, for exchanges including the News Server

Note that this exchange level information doesn't unequivocally catch more elevated level portrayals of action, like errands and objectives. Without tending to this need, it is unimaginable to expect to connect exchange level movement with resulting achievement or disappointment. Nor is it conceivable that exchange level investigation contains the way to more successful expert preparation (e.g., "you ought to utilize Internet Explorer more regularly.") Consequently, our underlying examination is focused around partner explicit test issues with the exchanges attempted to address them [10].

2.4 RECOGNIZING TASK-LEVEL ACTIVITY IN HUMAN/COMPUTER TRANSACTIONS:

Beginning information examination zeroed in on parsing information logs from the Tracer FIRE practice into significant blocks of time in which members were focused on a particular mid-level to undeniable level objective. Inside the setting of the Tracer FIRE work out, these undeniable level objectives would freely guide to the singular difficulties. While blocks of time could be characterized in view of the times in which difficulties were opened and when a response was submitted, there would be downsides to this methodology. For instance, members might work in a joint effort with different colleagues themselves getting to the game server. Moreover, members could enjoy broadened reprieves during which there is no movement related with a test. At last, the systems for parsing log passages into blocks of time during which members are focused on unambiguous undeniable level goals would be appropriate to settings stretching out past post-occasion investigation of Tracer FIRE practices and be generalizable to functional settings. In parsing signs into blocks of action, the main condition included times of latency. It was expected that a time of 15 minutes or more with no movement addressed a limit between two blocks. The one exemption for this standard tended to circumstance in which no exercises are logged on the grounds that the member is perusing material got to via looking through the Web. Likewise, when times of idleness of as long as 30 minutes were noticed and the latency was quickly gone before by activities reliable with the member getting to understanding material (e.g., Firefox followed by Adobe reader consistent with downloading and reading a pdf record), the period of inactivity didn't act as a parcel between blocks.

As portrayed beforehand, challenges were gotten to through a game server. At the point when a member opened a test, the activity showed up in the log as a "Set" occasion. In like manner, when a member presented a response, the activity was kept in the log as an "Accommodation" and when they deserted a test, the log recorded a "Leave." Exercises happening before a Set occasion were excluded from the block of exercises with the Set occasion, with it for the most part expected that a Set occasion (i.e., opening a test) addressed the start of a grouping of related exercises. Nonetheless, there were three special cases for this standard. In the first place, if a member had recently dealt with a test or one more colleague chipped away at a test, the member could be aware and pursue the answer for a test without opening the test. Inside the logs, this present circumstance was reflected by occasions in which there was a Set occasion promptly followed by an Accommodation. In these cases, the block of movement could reach out to incorporate exercises preceding the Set occasion. Second, in tackling a test, the response could be kept in an application like Notebook or WordPad or require the member to get to another product application (e.g., copy & paste a URL from Firefox). Subsequently, a Set and Submit occasion would be isolated by different exercises. To tends to these circumstances, a standard was embraced that whenever Set and Submit occasions were isolated by 3 or less activities, the block of action could start preceding the Set occasion. Third, members would frequently make a wrong accommodation for a particular test and before long, make another accommodation. Some of the time, this elaborate making minor alterations to their response (e.g., changing the linguistic structure) and different times, extra work was finished. In the logs, these circumstances showed up as Set and Submit occasions including the very challenge that were either progressive or isolated by different exercises. For this case, when there were various Set and Submit occasions including a similar 5092 Robert G. Abbott et al. /Procedia Assembling 3 (2015) 5088 - 5094 test, it was assumed that each Set occasion related to a continuation of going before work on the test, bringing about blocks of action that incorporated different Set occasions.

Accommodation of a right response was viewed as the finish of a block of exercises. Moreover, surrender of a test followed by opening an alternate test was viewed as the finish of a block of exercises. While News things gave the setting outlining the singular difficulties, they by and large didn't straightforwardly address the difficulties. News occasions were pushed to members, with members allowed to get to the News server to recover the news things at their tact. It is unlikely that a participant would go to the News server to search for data to use in settling a particular test, yet rather occasionally look at news things to check whether there was anything of interest. Occasions related with getting to the News server were excluded inside blocks of movement. Meetings started with a progression of exercises related with designing the PCs utilized by members and confirming their activity with these exercises kept in the logs. These exercises commonly elaborate order line exercises (i.e., cmd.exe) and use Windows Explorer, as well as Web programs to download programming or different documents [13]. Exercises toward the start of meetings were excluded from the examination if they included utilization of the order line joined by Windows Explorer or Internet Browser. Exercises including Hyperion, which is the product that upholds the assortment of information logs, were barred. Similarly, occasions in which members participated in exercises that plainly didn't connect with tackling the difficulties (e.g., game play with Minesweeper), and adjoining possibly related exercises were excluded from the examination of the information logs [10].

III. CYBERSECURITY TRAINING STRATEGIES FOR COMPREHENSIVE ORGANIZATIONAL DEFENCE

3.1. EMPLOYEE TRAINING

Organizations can utilize general cybersecurity training sites to instruct their workers about normal digital dangers, for example, phishing attack, malware, and social engineering techniques. This aides in making a culture of security awareness within the organization [14].

3.2. TECHNICAL STAFF DEVELOPMENT

For technical staff, companies can use specialized cybersecurity training sites that offers seminars on topics like penetration testing, network security, and incident response. This aides in improving the skills of IT experts responsible for securing the organization's infrastructure [15].

3.3. COMPLIANCE REQUIREMENTS

A few industries have specific cybersecurity compliance requirements, for example, HIPAA for medical services or PCI DSS for payment card industry. Organizations can use training sites that focuses on these compliance standards to guarantee their employees understand the regulatory requirements and how to comply with them [16].

3.4. VENDOR & PARTNER TRAINING

Organizations frequently collaborate with vendors and partners who might access their system or data. Giving admittance to network safety preparing locales for these external parties guarantees they understand the organization's security policies and procedures, reducing the risk of security incidents originating from third-party connections [17].

3.5. EXECUTIVE EDUCATION

Executives and senior management should know about cybersecurity risks and best practices to make informed decisions about network safety ventures and techniques. Specialized training sites customized for executives can provide them with the information they need to understand cybersecurity issues at an essential level [18].

3.6. INCIDENT ESPONSE PREPAREDNESS

Cybersecurity training sites that offer stimulated cyber-attack scenarios can assist organizations with preparing their incident response team to effectively detect, respond to, and mitigate security incidents. This hands-on training prepares the team for real-world cyber dangers and guarantees a prompt and coordinated response when an incident occurs [19].

IV. FINDINGS

4.1. PLURALSIGHT

- **Course Diversity:** Offers a wide range of cybersecurity courses covering topics from basic concepts to advanced techniques [20].
- **Quality of Content:** Provides high-quality, expert-led content with hands-on labs and assessments.
- **Interactive Features:** Incorporates interactive exercises and real-world scenarios to reinforce learning [21].
- **User Experience:** Intuitive platform with personalized learning paths and progress tracking.
- **Certification Options:** Provides skill assessments and certification paths for various cybersecurity domains [22].
- **Value for Money:** Offers subscription-based pricing with access to a vast library of courses, making it cost-effective for both individuals and enterprises.

4.2. CYBRARY

- **Course Diversity:** Extensive catalogue of cybersecurity courses, including both free and premium options [23].
- **Quality of Content:** Varied content quality, ranging from beginner-friendly to more advanced topics.
- **Interactive Features:** Limited interactive elements but includes virtual labs for hands-on practice [24].
- **User Experience:** Simple interface but lacks personalized learning paths and progress tracking.
- **Certification Options:** Offers certification preparation courses and skill assessments [25].
- **Value for Money:** Free tier available, with premium subscription offering additional features and content.

4.3. UDEMY

- **Course Diversity:** Wide array of cybersecurity courses taught by industry professionals [26].
- **Quality of Content:** Varies depending on the instructor, with some courses offering high-quality content while others may lack depth [27].
- **Interactive Features:** Limited interactive elements, primarily video-based lectures [28].
- **User Experience**: User-friendly interface with course reviews and ratings for guidance [29].
- **Certification Options:** Provides courses for various cybersecurity certifications, but certification exam fees are not included [30].
- **Value for Money:** Courses available for individual purchase, offering flexibility but potentially higher costs for multiple courses.

V. SUMMARY & CONCLUSION

Cybersecurity training is crucial for equipping IT professionals to handle increasing online threats. Traditional platforms like Capture The Flag (CTF) offer basic tasks without virtual network environments, whereas recent open-source platforms provide realistic training environments. Human errors often lead to significant cyberattacks, highlighting the need for comprehensive cybersecurity training covering content representation, environmental management, and training facilitation.

This study involved two Tracer FIRE cybersecurity training exercises conducted in 2014, with a total of 26 participants—11 in the spring and 15 in the summer. The exercises featured multi-day events that combined classroom instruction on cybersecurity tools and techniques with team-based competitive challenges. Participants, who consented to data collection, had their human-machine interactions logged automatically during these exercises. Each participant used a computer equipped with essential cybersecurity software, and a game server managed the challenges and submissions. Data logs captured various types of interactions, such as keystrokes and software use, and were parsed into meaningful activity blocks to identify task-level goals and performance. This parsing considered periods of inactivity and the sequence of challenge-related actions to create a comprehensive record of each participant's activities. The analysis aimed to associate specific problem-solving actions with overall performance, excluding irrelevant activities to focus on relevant cybersecurity tasks.

To build a comprehensive organizational defense, various cybersecurity training strategies can be implemented. General employee training on common cyber threats like phishing, malware, and social engineering fosters a culture of security awareness. Specialized training for technical staff enhances skills in areas such as penetration testing, network security, and incident response. Compliance-focused training ensures employees understand industry-specific regulatory requirements like HIPAA or PCI DSS. Vendor and partner training on the organization's security policies reduces risks from third-party connections. Executive education provides senior management with the knowledge to make informed cybersecurity decisions. Finally, incident response preparedness through simulated cyber-attack scenarios equips teams to handle real-world threats effectively.

The findings compare three cybersecurity training platforms: Pluralsight, Cybrary, and Udemy. Pluralsight offers a diverse range of high-quality, expert-led courses with interactive features and personalized learning paths, making it user-friendly and cost-effective through a subscription model. Cybrary provides an extensive catalogue of free and premium courses with varied content quality, limited interactive elements, and a simple interface, offering good value with a free tier and premium options. Udemy features a wide array of courses with variable quality, limited interactivity, and a user-friendly interface, allowing for individual course purchases, which can be flexible but costly for multiple courses.

In conclusion, comprehensive cybersecurity training is vital for equipping the IT workforce with the skills to counteract the increasing threats posed by cyberattacks. Effective training platforms must balance content delivery, environmental management, and training facilitation to ensure thorough learning. The findings demonstrate that platforms like Pluralsight, Cybrary, and Udemy offer varied strengths. Pluralsight excels in course diversity, quality, and interactive features, making it a cost-effective choice for organizations. Cybrary provides a broad range of courses with both free and premium options, although it has limited interactive elements. Udemy offers flexible course purchasing with varying content quality and limited interactivity. Each platform has its own advantages, making them suitable for different organizational needs and budgets. Emphasizing the need for targeted training for employees, technical staff, executives, and third-party partners, alongside robust incident response preparedness, will bolster an organization's cybersecurity defences effectively.

VI. ACKNOWLEDGEMENT

We extend our gratitude to the academic community, researchers, scholars, participants, and institutional support for their contributions to this paper. Their invaluable assistance and support have been instrumental in its completion**.**

REFERENCES

[1] Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636. https://doi.org/10.1016/j.cose.2019.101636

[2] Švábenský, V., Čeleda, P., Vykopal, J. and Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security, 102, p.102154. doi: https://doi.org/10.1016/j.cose.2020.102154.

[3] Beuran, R., Chinen, K.-I., Tan, Y. and Shinoda, Y. (n.d.). Towards Effective Cybersecurity Education and Training. [online] Available at: https://www.jaist.ac.jp/~razvan/publications/effective_cybersecurity.pdf.

[4] GOV.UK. (n.d.). Educational institutions findings annex - Cyber Security Breaches Survey 2022. [online] Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022.

[5] Abawajy, J. (n.d.). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, [online] 33(3), pp.237–248. Available at: https://www.academia.edu/20452374/User_preference_of_cyber_security_awareness_delivery_methods.

[6] Dihoff, R. E., Brosvic, G. M., Epstein, M. L., & Cook, M. J. (2004). Provision of feedback during preparation for academic testing: Learning is enhanced by immediate but not delayed feedback. Psychological Record/˜ the œPsychological Record, 54(2), 207–231. https://doi.org/10.1007/bf03395471

[7] Prümmer, J., van Steen, T. and van den Berg, B. (2023). A systematic review of current cybersecurity training methods. Computers & Security, [online] 136, p.103585. doi: https://doi.org/10.1016/j.cose.2023.103585.

[8] Beuran, R., Pham, C., Tang, D., Chinen, K.-I., Tan, Y. and Shinoda, Y. (n.d.). CyTrONE: An Integrated Cybersecurity Training Framework. [online] Available at: https://www.jaist.ac.jp/~razvan/publications/cytrone_integrated_framework.pdf [Accessed 23 May 2024].

[9] Beuran, R., Vykopal, J., Belajová, D., Čeleda, P., Tan, Y. and Shinoda, Y. (2023). Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms. Computers & Security, [online] 128, p.103120. doi: https://doi.org/10.1016/j.cose.2023.103120.

[10] Abbott, R.G., McClain, J., Anderson, B., Nauer, K., Silva, A. and Forsythe, C. (2015). Log Analysis of Cyber Security Training Exercises. Procedia Manufacturing, 3, pp.5088–5094. doi: https://doi.org/10.1016/j.promfg.2015.07.523.

[11] Abbott, R. G., McClain, J. T., Anderson, B., & Forsythe, C. (2015). Automated performance assessment in cyber training exercises. ResearchGate. https://www.researchgate.net/publication/281638958_Automated_Performance_Assessment_in_Cyber_Training_Exercises

[12] McClain, J.T., Silva, A.R., Avina, G.E. and Forsythe, J.C. (2015). Measuring Human Performance within Computer Security Incident Response Teams. [online] www.osti.gov. Available at: https://www.osti.gov/servlets/purl/1226116.

[13] Veeraraghavan, S. (2017). Best Programming Languages | Most Popular Languages to Learn – Simplilearn. [online] Simplilearn.com. Available at: https://www.simplilearn.com/best-programming-languages-start-learning-today-article.

[14] Qawasmeh, S. A., Alqahtani, A. a. S., & Khan, M. K. (2024). Navigating Cybersecurity Training: A Comprehensive review. ResearchGate. https://www.researchgate.net/publication/377557574_Navigating_Cybersecurity_Training_A_Comprehensive_Review

[15] Daniel, C., Mullarkey, M. and Agrawal, M. (2022). RQ Labs: A Cybersecurity Workforce Skills Development Framework. Information Systems Frontiers. doi: https://doi.org/10.1007/s10796-022-10332-y.

[16] Hijji, M. and Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, [online] 22(22), p.8663. doi: https://doi.org/10.3390/s22228663.

[17] Ghazvini, A. and Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. International Journal of Advanced Computer Science and Applications, 7(5). doi: https://doi.org/10.14569/ijacsa.2016.070549.

[18] Mathur, A. (2024). Incident Response Simulation Framework. Indian Scientific Journal of Research in Engineering and Management, 08(04), 1–5. https://doi.org/10.55041/ijsrem31743

[19] O'neil, A., Ahmad, A. and Maynard, S. (n.d.). Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training. [online] Available at: https://arxiv.org/pdf/2108.04996.

[20] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12), 2175. https://doi.org/10.3390/sym15122175

[21] M, D. K., & Jena, S. R. (2024). Defensive Cyberspace: Navigating the landscape of cyber security. ResearchGate. https://doi.org/10.5281/zenodo.10529045

[22] Léger, M. (2023). The competency requirements of cybersecurity professionals in Canadian financial sector organizations. ResearchGate. https://www.researchgate.net/publication/371173313_The_competency_requirements_of_cybersecurity_professionals_in_Canadian_financial_sector_organizations

[23] Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

[24] Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181

[25] González-Manzano, L., & De Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. Computers & Security, 80, 238–256. https://doi.org/10.1016/j.cose.2018.09.009

[26] Lastname, F., & Rehman, I. U. (2023). Cybersecurity education training techniques: A systematic literature review. ResearchGate. https://doi.org/10.13140/RG.2.2.17199.71849

[27] Tigina, M., Birillo, A., Golubev, Y., & Bryksin, T. (2023). Analyzing the quality of submissions in online programming courses. ResearchGate. https://www.researchgate.net/publication/367462232_Analyzing_the_Quality_of_Submissions_in_Online_Programming_Courses

[28] Qiu, R. (2020). Udemy: Blended and E-Learning for Transforming Teaching and Learning. In Education in the Asia-Pacific region (pp. 215–220). https://doi.org/10.1007/978-981-15-7018-6_26

[29] Alojaiman, B. (2021). Toward selection of trustworthy and efficient E-Learning platform. IEEE Access, 9, 133889–133901. https://doi.org/10.1109/access.2021.3114150

[30] Blažič, B. J. (2021). Cybersecurity Skills in EU: New educational concept for closing the missing workforce gap. In IntechOpen eBooks. https://doi.org/10.5772/intechopen.97094