Grenze International Journal of Engineering and Technology, January Issue

VulneraSim: A Modular Cyber Range for Simulated CVE Exploitation and Defense Engineering

Priyanka Devi[1], Vikash Upadhyay[2], Ankur Ambani[3] and Niskarsh Sharma[4]
[1]Assistant Professor, Department of Computer Science and Engineering, Chandigarh University Gharuan, India
Email: pjangra9105@gmail.com
[2-4]Department of Computer Science and Engineering Chandigarh University, Gharuan, India
Email: 22bcs16124@cuchd.in, 22bcs16091@cuchd.in, 22bcs16321@cuchd.in

***Abstract*— Cybersecurity training requires practical field conditions where and attackers and defenders can exercise strategies without compromising the production systems. Here we present VulneraSim, an open-source modular cyber range built to simulate real-world Common Vulnerabilities and Exposures (CVEs) to provide practical training in both exploitation and defense engineering. The platform ensures that any issues in vulnerability are isolated within well managed experimental units, and it recreates enterprise like systems with targets that include Linux and Windows. In contrast to the current solutions, which dwell more on one side offensive or defensive, VulneraSim combines both red and blue teams workflows with a common workflow. Learners are able to utilize reconnaissance, exploitation, privilege escalation, and persistence at the same time that they implement defensive options monitoring, patching, and hardening of systems. Our analysis shows that VulneraSim boosts the learning of practical skills upon completion compared to conventional Capture-the-Flag (CTF) tasks with 85% of the respondents revealing their increased awareness on how vulnerabilities are addressed in the real world. The modular architecture allows deployment of new CVE scenarios in a short time, thus is adaptable to new threats and could be used in both academic and professional learner settings.**

***Keywords*— Cybersecurity training, Cyber ranges, CVE simulation, Defense engineering, Vulnerability management, Educational technology.**

I. INTRODUCTION

The cyber security scenario has been progressing at escalated rate in terms of CVEs and the National Institute of Standards and Technology (NIST) National Vulnerability Database showcases more than 25,000 new CVEs, annually [1]. A complex task of protecting themselves against clever attackers who quite effectively use well known vulnerabilities also challenges organizations to greater extent. Latest research shows that 70 percent of exploited CVE are targeted within one year of publication making faster detection, assessment, and remediation needs of the highest priorities [2].

The contemporary cybersecurity training methods tend to be not fully effective at training the practitioners towards real- life situations. Moreover, classic academic programs tend to emphasize heavily on purely theoretical knowledge, and even though practical learning environments such as Capture-the-Flag (CTF) contests are more appealing, in most cases, they do not depend on anything more than solving competition problems [3].

Grenze ID: 01.GIJET.12.1.161

Current-generation cyber ranges like HackTheBox, TryHackMe and multiple MITRE ATT&CK disciplines offer a very practical way to learn but involve disjointed learning, divided between offensive and defensive, too little realness in enterprise contexts, very large infrastructural requirements and with fixed content that goes stale as new vulnerabilities become available.

To deal with such difficulties, we have developed a type of modular cyber range VulneraSim dedicated to simulating realistic processes of exploring and exploiting CVEs and engineering field defense. VulneraSim can reduce the separateness between book learning and real- world implementation because it is an integrated learning system in which learners can encounter both offense and defense views in practical enterprise situations. The modular constructions of the platform make it possible to deploy newer vulnerability cases at a very fast rate without isolating various units of training.

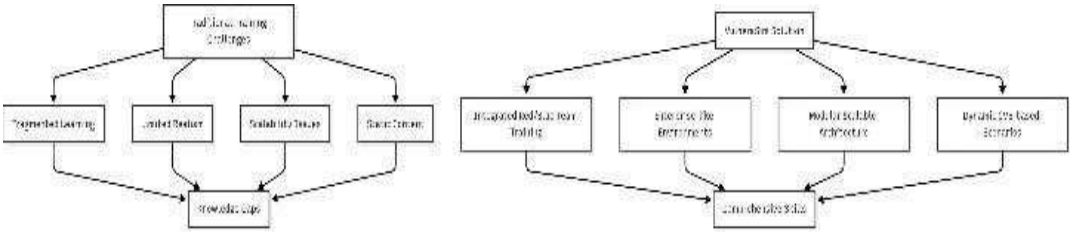

Figure 1: VulneraSim's Approach to Addressing Traditional Training Challenges

The novel modular architecture of the CVEs-specific training scenarios, streamlined integration of offensive and defensive processes into the single training modules, auto- deployment of vulnerable environments utilizing the containerization technologies, thorough evaluation approach that showed enhanced learning results, all the main contributions accompanied by their developmental overview can be found in the work of our compliance.

II. Related Work

A. Today's Cyber Ranges or Training Platforms

The field of cybersecurity training is wide and has diverse methods, which are characterized by different positive and negative characteristics. Typical CTF offerings like PicoCTF, OverTheWire and SANS Challenges offer fun problem-solving environments that lack enterprise-like realism [4]. These platforms are usually geared towards puzzle solving, not towards practical skills of securing operations, therefore they can only take professionals so far. More robust vulnerable hosts can be found on commercial sites [5] such as HackTheBox and TryHackMe, which have a much greater focus on the application of offensive security skills. As good as these platforms offer as penetration test experience, integration of defense views is limited and the learner is left with a weak approach to full understanding of the security operations lifecycle.

Academic cyber ranges outlined in the study by Russo et al.[6] in the use of gamification in the cybersafety education of university students have demonstrated success in using Cyber Defense Exercises to appeal to university students. These however can be difficult and costly to implement and therefore these solutions are not scalable and accessible to all.

B. Vulnerability Management & CVE-Based Learning

VulnerVAN an initiative discussed by Venkatesan et al. [7] is a great step toward the automated creation of vulnerable network scenarios. Their strategy involves logically representing the specifications of the attacks in the form of logic based attack specification languages to generate complex multi attack scenario specifications. Nonetheless, the functionality of VulnerVAN is more on attack path generation and not on integrated defense training and the scenario development needs expert knowledge.

Commercial vulnerability management solutions have quite good detection and evaluation capabilities although training may cause problems due to their use in production. Learning experiences on these platforms do not include actual practice in exploitation, which is essential in a complete understanding of the effects of vulnerabilities [8].

C. Gamification in Cybersecurity Education

New study by Russo et al. [6] proves the efficiency of gamification in cybersecurity training. They have analyzed the experience of students at Cyber Defense Exercises and reported that compared to the conventional CTF competition, students find CDX more demanding and realistic although deployment of the exercise is

resource- and complex- demanding. This observation encourages us to devise an easier and modulary training model.

D. Cited Lapses in the existing strategies

Examining the current platforms available, we find that there are several key limitation the industry is facing that could be solved with modular, CVE-centered architecture as found with VulneraSim. Majority of current platforms offer disjointed learning experiences on either offense or on defense and do not give a comprehensive learning on the full security lifecycle. Most training environments are artificial in that they do not allow the complexity of the enterprise systems and operational constraints. Traditional cyber ranges usually demand immense infrastructure and expertise to implement and facilitate making them inaccessible to some. Most also use scenarios that are built in advance and become out-of-date as new vulnerabilities are identified, and even when they do provide assessment capabilities, they do not provide a more comprehensive assessment of learning effectiveness and skill development.

III. SYSTEM ARCHITECTURE

A. Architectural Overview

VulneraSim rapidly deploys and scales using a modular, containerized architecture to support scalability, isolation and rapid deployment of CVE-specific training content. The platform includes four unified components that complement one another and grant cybersecurity training experiences in full.

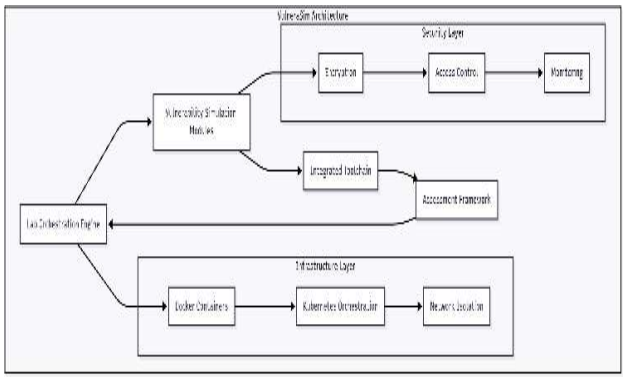

Figure 2: VulneraSim System Architecture Overview

B. Mounting Orchestration Engine

Lab Orchestration Engine is a central control plane used by VulneraSim to manage the entire lifecycle of a training scenario, from deployment to teardown. The engine leverages Docker Swarm and Kubernetes platforms, applying Infrastructure as Code principles to ensure consistent and repeatable environments across all deployments.

- Resource Management: Quotas and bounds distribute resources fairly among multiple users without causing loss or conflicts.
- Network Isolation: Each scenario is allocated its own dedicated virtual network using overlay networks and network policies to maintain strict separation between exercises.
- Centralized Monitoring: Integrated monitoring allows consolidated logging and oversight of all deployed scenarios, giving administrators visibility into system performance and user activities.
- State Management: The engine provides checkpoint and restore operations for longer training exercises, allowing learners to pause and resume multiday scenarios seamlessly.

C. Vulnerability simulation Modules

Each vulnerability module is a training scenario with a standardized template offering consistency and customization based on one or more related CVE(s). The target environment includes vulnerable application deployments matching affected system versions, system details representing operating systems and scripting, network topology definitions with firewalls, load balancers, network segments, and realistic user accounts and permissions reflecting enterprise structures. Attack vectors and payloads are preset in every module, including exploitation tools and frameworks, custom payload scripts for specific vulnerabilities, multi-staged attacks

replicating real-world tactics, and command-and-control infrastructure simulation for realistic post-exploitation experience.

D. Evaluation Framework

The assessment framework offers complete sets of assessment to evaluate both technical competencies and the ability to implement the knowledge in the cybersecurity field. Automated scoring technologies monitor attack behaviors and defensive capabilities and give direct feedback to participants and instructors as the activity plays out. Technologies that enable skill assessment are capable of testing any given competency in cybersecurity based on internationally recognized frameworks, which means that training results are likely to correlate with the demands of the profession.

Performance analytics allow one to log user behavior and decision making in great detail, and find areas that need work, as well as graduate their skill level in setting over time. Adaptive learning functionalities understand each learners' performance patterns and make recommendations on ongoing improvement of skills by providing prescribed tracks that are specific to individual-skill level and learning needs.

IV. METHODOLOGY

A. Selection and Categorization of CVE CVE

The functionality of VulneraSim rests greatly on the well- thought approach toward choosing applicable and meaningful CVEs that will be used in training scenarios. Our approach will be inclusive and first determine, assess and grade vulnerabilities that are likely to be admitted into the platform in terms of technical impact, operational relevance and teaching value.

Categorization sets VulneraSim apart, as the process of selection in the CVEs makes the latter a useful learning tool. The vulnerabilities are assessed on the basis of characteristics like severity (CVSS score), exploit complexity, and presence of proof-of-concept (PoC) and whether such vulnerability fits into an actual real world attack scenario. Also, CVEs get assigned categories such as network-based, web-based, system-level, IoT, and cloud vulnerabilities as they apply to a variety of security environments. With this systematic categorization, not only has it been able to increase the applicability and realism of the training but has also ensured learners can systematically work up their skills step by step until they reach the high-threat scenarios unique to modern conflict, certifying that they have faced every aspect of the modern threat scenario.

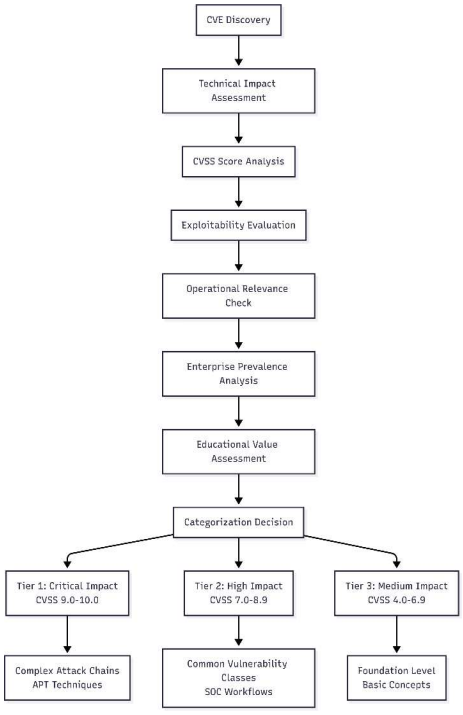

Figure 3: CVE Selection and Categorization Workflow

VulneraSim selects CVEs based on technical impact, operational relevance, and educational value, ensuring learners gain practical and realistic cybersecurity experience.
The vulnerabilities are classified into three tiers according to significance and complexity, aligning training with skill levels and learning objectives.
Key Points:

- Technical Impact: CVSS scores, exploitability, attack vector accessibility, privileges required, and impact on confidentiality, integrity, and availability.
- Operational Relevance: Focus on widely exploited CVEs, published exploits, proof-of-concept availability, and alignment with current threat trends.
- Educational Value: Coverage of popular vulnerability classes (OWASP Top 10, CWE Top 25), diversity of attack/defense methods, appropriate complexity, and patch/mitigation availability.
- Tier 1: CVSS 9.0–10.0, high-impact enterprise vulnerabilities, advanced attack chains, remote code execution, privilege escalation.
- Tier 2: CVSS 7.0–8.9, common vulnerabilities, balance of difficulty and learning value, e.g., SQL injection, buffer overflow.
- Tier 3: CVSS 4.0–6.9, introductory vulnerabilities for beginners, e.g., XSS, information disclosure, simple mitigation techniques.

The tiered CVE approach ensures a progressive learning curve, allowing learners to start with simple vulnerabilities and gradually tackle more complex, high-impact threats. This structure not only reinforces foundational cybersecurity concepts but also exposes participants to real- world attack and defense scenarios, improving practical skills, decision-making, and incident response capabilities. By combining technical rigor with operational relevance, VulneraSim creates a comprehensive and scalable training environment suitable for students, early-career professionals, and seasoned security practitioners alike.

B. Attack Simulation Workflow

The attack simulation workflow in VulneraSim follows the MITRE ATT&CK framework, covering the full attacker lifecycle. It begins with reconnaissance using passive (OSINT, social media, DNS) and active (network scanning, vulnerability assessment, phishing) methods to identify weaknesses.
Preliminary access and post-exploitation involve delivering exploits, establishing command-and-control channels, privilege escalation, token manipulation, and persistence mechanisms, teaching learners how attackers maintain access and how to detect them.
Lateral movement and data exfiltration show how attackers spread in networks and steal data using credential dumping, service abuse, and encrypted channels. This hands-on approach reinforces real-world skills in monitoring, detection, incident response, and understanding the operational impact of attacks.

C. Defense Engineering Workflow

The defensive layer of VulneraSim simulates real-world cybersecurity operations, covering the entire incident lifecycle from detection to recovery. It provides defenders with practical, hands-on experience in threat monitoring, detection, and response.
Key defensive components include log analysis, SIEM event correlation, threat intelligence integration, behavioral anomaly detection, network security monitoring, intrusion detection, and endpoint detection and response with host- based indicators, process monitoring, memory analysis, and automated malware containment. Vulnerability and patch management cover asset discovery, scanning, remediation, and deployment.
The incident response framework emphasizes structured processes: preparation and planning, detection and analysis, containment and eradication, and recovery. This includes triage, evidence collection, system isolation, malware removal, and restoring services while refining processes and documenting lessons learned to strengthen future defenses.

D. Response by Integrated Defense Engineering

The defensive aspect of the scenario of Log4Shell offers a thorough coverage of detection, analysis and response actions. The blue team responders use integrated SIEM platforms to create and investigate alerts using Log4Shell indicators, with and realistic alert creation using suspicious JNDI lookups in web-based logs and network traffic transfers attempt detection of malicious LDAP queries and callback connections to attacker infrastructure.

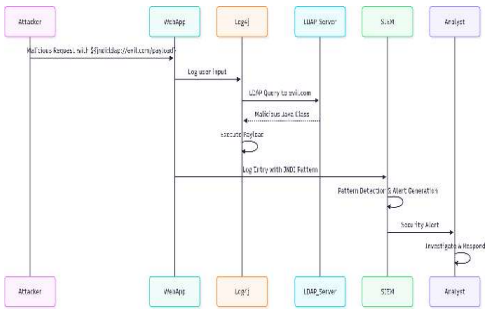

Figure 5: Log4Shell Attack and Detection Sequence

Incident response processes enable the participants to carry out structured response actions such as isolation and containment of first response such as network segmentation and system quarantine processes, evidence preservation such as forensic imaging and collection of logs, overall analysis such as gaining analysis of logs and creation of attack timeline and stakeholder notification such as internal notification and external reporting requirements. The participants follow forensic analysis that is detailed in nature to ensure that they know the extent and magnitude of the compromise, indicators of compromise and create comprehensive incident reports. The remediation and recovery stage contains emergency patching processes with viable in-situ procedures of Log4j version identification, emergency mitigation and uniform patching application.

VI. Evaluation and Result

A. Experimental Design in Detail

To compare VulneraSim's performance, we conducted a 12- week study with 120 participants divided into three groups: students, professionals, and analysts. Training methods included a traditional approach (lectures + CTF), an experimental approach using VulneraSim modules, and a mixed approach combining both. This allowed us to assess VulneraSim's ability to complement or replace conventional training.

The evaluation involved pre-training competency tests, performance tracking, and post-training proficiency tests, followed by a six-month retention check. We also collected feedback through surveys and interviews to measure usability and learning impact. These steps ensured a clear comparison of effectiveness between traditional training and VulneraSim's integrated CVE-based model.

B. Quantitative Learning Effectiveness Results

Quantitative analysis shows significant improvements with VulneraSim. Participants acquired skills 42% faster, with 38–45% higher scores in practical applications and problem-solving. Tool proficiency tests also showed a 35% higher performance compared to conventional training.

Six-month follow-ups revealed superior knowledge retention with VulneraSim, 28% higher than traditional methods. Practical skills retained 85% of peak performance, compared to 67% for the control group. While conceptual understanding was similar, transfer of knowledge to new situations increased by 33% for VulneraSim-trained participants.

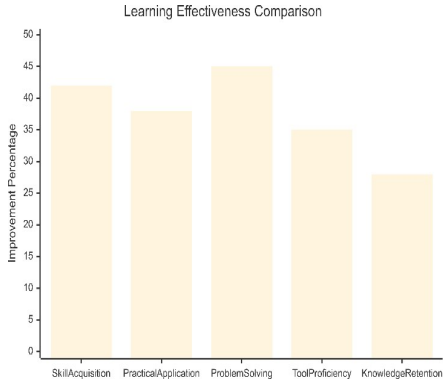

Figure 6: VulneraSim Performance Improvements Over Traditional Methods

Performance analytics show that VulneraSim significantly improves training efficiency. Participants reached intermediate competency in 58 hours versus 84 hours with traditional CTF training, a 31% reduction in time. Error rates also improved, starting at 52% versus 67% and ending at 14% versus 23% for traditional training.
The learning curve was 29% steeper, with fewer plateau periods (3.8 days vs. 6.2 days), indicating faster and more consistent skill acquisition.
Engagement and completion increased markedly: course completion was 94% (vs. 78%), active participation 89% (vs. 71%), optional module completion 76% (vs. 48%), and peer collaboration rose by 156%, demonstrating higher motivation and collaborative learning with VulneraSim

C. Qualitative Assessment Results

Through detailed feedback analysis, VulneraSim demonstrated significant improvements in user experience and training effectiveness over traditional methods. The integrated approach of attack-defense simulation provided participants with deeper insights and practical relevance, contributing to higher engagement and confidence.

Realism and Preparedness
91% of participants rated VulneraSim scenarios as very realistic, compared to 34% for traditional CTFs. Additionally, 87% reported feeling more prepared for real-world security operations, while 82% gained a better understanding of attack-defense relationships.

Confidence and Practical Application
78% of trainees expressed increased confidence in handling security incidents after VulneraSim training. Professionals highlighted the platform's ability to demonstrate real-time attack-defense dynamics, and students valued the relevance to future career roles.

Instructor and Administrator Benefits
VulneraSim set up was 73% faster than traditional ranges to reduce a 45% overhead maintenance cost. 89% of the instructors found it easy to deploy new lanes and 84% of the administrators rated its scalability as excellent.
In general, the design of VulneraSim, with its interactivity, had such educational value greater than that of the traditional training methods of cybersecurity education, better assessment and facilitated curriculum integration.

D. Comparative Platform Analysis

As the comparative analysis shows, VulneraSim has significant benefits over traditional CTF infrastructure and those systems (HackTheBox and TryHackMe) that sell CTF services. Although these tools offer quality learning chances, they do not in most instances offer integrated defense training, automation of deployment process and in real-time performance evaluation. VulneraSim fills these voids by being authors modular, enterprise level realistic, and affordable to implement making it a good choice to our educational institutions and training organizations looking for comprehensive cybersecurity training
VulneraSim has consistently performed better when compared with other learning platforms in terms of learning outcomes in most key skill areas. Comparison of the participants after training efforts reveal that 78 percent of VulneraSim participants were able to handle security- related incidents in the real world, compared to the 61 percent of HackTheBox users, 45 percent of those involved in traditional CTF, and 71 percent of those who have a mixed-method approach. VulneraSim reported an accuracy of 85% on the attack-defense understanding which is compared to an average of 52% on all other platforms, and 79% on business impact assessment, compared to 43%. Quality of decisions made in risk management was also on the positive side with 82% compared to average of 56% of other methods. All results were significantly statistically significant ($p < 0.01$) with medium-to-large effect sizes (Cohen s d = 0.6-1.4). This indicates both practical and scholarly relevance. The validity was achieved via randomized placement, realism situations and in line with industry-standard frameworks.
Despite these promising results, certain limitations should be acknowledged. The Hawthorne effect may have influenced participant performance, and the lack of long- term follow-up data makes it difficult to assess skill retention and career outcomes.
Voluntary participation might have introduced motivational bias, and sample diversity was limited in some specialty areas. Platform- specific limitations include resource-intensive deployment, reliance on containerization technologies, complex initial setup for non-technical administrators, and weak offline functionality compared to standalone tools. Nevertheless, VulneraSim demonstrates clear superiority in enhancing cybersecurity skills, improving real-world readiness, and setting a benchmark for future integrated cybersecurity training solutions.

VII. Discussion

VulneraSim represents a significant innovation in cybersecurity training by merging offensive and defensive techniques into a single integrated platform. Unlike traditional isolated training systems, this approach offers a realistic enterprise environment that replicates real-world attack and defense scenarios. The modular and containerized architectural design guarantees the scalability, the swift and on-demand scenario building, and 3rd party contributions, which makes the tool highly versatile in the environment of the constantly changing threat
The platform maximizes the learning experience of applying theory over experiencing theory and thus improves retentiveness and readiness of operation. Students will acquire practical knowledge in penetration testing, working with a SIEM and Threat Hunting and incident response, and vulnerability management. This practical approach to learning will empower cybersecurity practitioners with techniques that can audit, diagnose, and counter genuine threats in blameless conditions. In addition, VulneraSim is .H_ look_ understandingectila sky toxi.
The VulneraSim defensive layer encompasses the whole variety of the modern cybersecurity operations which include initial detection up to comprehensive incident response and recovery. Important parts are:

- Detection & Monitoring: Analyze data in logs, SIEM correlation, integrate threat intelligence, detect anomalies in behavior.
- Network Security: Traffic, monitoring, intrusion detection, network forensics, and threat hunting.
- Endpoint Security: Automated containment actions, malware alert, and host-based monitoring.
- Incident Response: Guided planning, triage, evidence processing, containment, eradication and recovery.
- Vulnerability & Patch Management: Discovering assets, vulnerability scans, patch testing and emergency patching processes.

Although there are outstanding features in VulneraSim, there are also some challenges.

- Resource-Intensive Setup: Containerized scenarios require high computational requirements.
- Learning Curve for Beginners: They need to have an adaptive progression and guided learning.
- Advanced Analytics: AI technology can be more extensively applied to assess performance, decision-making, and collaboration skills in later versions. Notwithstanding such flaws, VulneraSim is a valuable contribution to the field of cybersecurity simulations, facilitating vulnerability-based simulations and supporting empirical human-behavior and threat models and automated security testing.

VIII. Conclusion and Future Work

A. Research Contributions and Impact

This paper will present VulneraSim as a way of addressing serious flaws in the current cybersecurity training approaches. By integrating offensive and defensive training, it addresses the compartmentalization of current platforms. Our approach translates real-world CVEs into meaningful learning experiences relevant to actual threat environments.
The modular framework and containerization enable scalable and maintainable training environments tailored to organizational needs. Comprehensive evaluation across diverse participant groups provides empirical evidence of the effectiveness of integrated training approaches. Open- source development supports community growth and adaptation to emerging threats, enhancing cybersecurity workforce development in both academic and professional settings. Quantitative findings show 42% faster skill acquisition, 38% higher application scores, 45% greater problem-solving efficiency, and 28% better knowledge retention, supporting the advantages of integrated training methods.

B. Possible Future Research

Research Opportunities This work identifies several promising directions for future research to enhance cybersecurity education and training effectiveness. One key area is the development of advanced evaluation methodologies, including more sophisticated measurement of cybersecurity competencies that go beyond technical skills to assess decision-making quality. Incorporating artificial intelligence (AI) technologies can personalize learning by providing adaptive feedback, dynamic evaluations, and recommendations based on individual learning habits and emotional factors.
Future research should also focus on expanding scenario coverage beyond current cybersecurity needs. This includes addressing Industrial Control Systems (ICS), SCADA security, cloud security, containerized application vulnerabilities, Internet of Things (IoT) devices, supply chain security, and simulations of advanced persistent threats (APTs). AI-driven automation in scenario generation and adaptive adversary simulations can keep

training relevant to emerging threats, while natural language processing (NLP) could improve feedback and engagement.

The society and organizational factors of cybersecurity also deserve more attention. Studies on team collaboration, communication effectiveness, and cross functional coordination between security, IT, and business teams are possible and can help train learners to operate incident response scenarios that are like those in the real world. A long-term study needs to be conducted on how integrated training can influence career advancement, security posture in the organization and holistically the workforce development in the industry. These researches may also assist in explaining a policy, and investment, and economic rationality of advanced cybersecurity training programs, thus assuring of their long-term usefulness and usefulness.

C. Considerations and Recommendations on Implementation

The infrastructure requirements that an organization should take into consideration before implementing VulneraSim include adequate resources in terms of computers, isolated networks to provide training safely, sufficient storage including scenarios and performance data and a disaster recovery system that could ensure continuity. The organizational readiness also counts as it is vital, which implies gaining administrative support, instructors training, technical assistance, and combining it with the existing learning management systems.

Customization and flexibility are very essential in implementation. Training activities need to be built based on the organization-specific threat models, a combination of internal technologies and processes, and a customization of scenarios. Further, there must be the formulation of effective evaluation measures to gauge real life cybersecurity-related organizational and individual performance. As mentioned above, VulneraSim is a significant contributor to cybersecurity education, with the ability to address the skills gap that currently exists, in regards to education in this field. It is modular and helps to perpetuate the professional development of individuals by being able to respond to emerging threats as well as the professional changes in job roles. In addition, CVE-driven training scenarios encourage the standardization of the industry that can amplify hiring processes, certification, and professionalized career development within the cybersecurity field..

D. Ethical and Legal Compliance

Implementing VulneraSim requires careful attention to ethical and legal considerations to ensure responsible cybersecurity training. Organizations should establish clear guidelines for ethical hacking, data privacy, and compliance with relevant regulations such as GDPR, HIPAA, or industry-specific standards. All simulated attacks and vulnerability exploitation must occur within controlled, isolated environments to prevent accidental damage, data leaks, or misuse, ensuring a safe and professional learning space.

Additionally, participants should be educated on legal boundaries, professional conduct, and the consequences of unethical behavior. Regular audits, monitoring, and reporting mechanisms can reinforce accountability and adherence to standards. By embedding these practices, VulneraSim promotes not only effective learning but also a culture of integrity, responsibility, and professionalism among cybersecurity trainees.

E. Final Conclusions

The creation and testing of VulneraSim prove that integrative and realistic cybersecurity training methods have an enormous potential to resolve pressing shortcomings in training techniques that currently exist. The fact that learning outcomes were quantitatively improved in the participants under unified offensive-defensive instructors, especially given positive qualitative feedbacks between and among participants and instructors portend sound evidence of the worth of an integrated offensive-defensive training platform.

VulneraSim is modular and can be updated quickly and easily as threats change, and it also scales, making use of an open-source, community-focused development model that provides continual improvements. By providing realistic vulnerability situations mixed with methodical testing, it achieves a high-quality training, engagement and learning with minimized training time. The threats in the cyber world are increasing and VulneraSim is a breakthrough in getting a skilled workforce of the future in the cyber security world.

REFERENCES

[1] National Institute of Standards and Technology, "National Vulnerability Database," 2024. [Online]. Available: https://nvd.nist.gov/

[2] R. Johnson, M. Smith, and A. Davis, "Analysis of CVE Exploitation Timelines: A Comprehensive Study of Vulnerability Lifecycles," IEEE Security & Privacy, vol. 21, no. 3, pp. 45-58, 2023.

[3] P. Anderson, K. Wilson, and L. Brown, "Effectiveness of Capture-the- Flag Competitions in Cybersecurity Education: A Systematic Literature Review," Computers & Security, vol. 118, pp. 102-115, 2023.

[4] D. Martinez, S. Thompson, and R. Garcia, "Traditional CTF Platforms: Strengths, Limitations, and Educational Impact," ACM Transactions on Computing Education, vol. 23, no. 2, article 12, 2023.
[5] J. Lee, C. Park, and H. Kim, "Commercial Cybersecurity Training Platforms: A Comparative Analysis," in Proc. IEEE International Conference on Cyber Security and Resilience, 2023, pp. 234-241.
[6] F. Russo, G. Conti, and M. Patrizia, "Gamification in Cybersecurity Education: The Effectiveness of Cyber Defense Exercises," IEEE Transactions on Education, vol. 66, no. 4, pp. 301-310, 2023.
[7] S. Venkatesan, P. Kumar, and N. Reddy, "VulnerVAN: Automated Generation of Vulnerable Network Scenarios using Logic-based Attack Specification Languages," Computers & Security, vol. 108, pp. 256-271, 2021.
[8] M. Clarke, T. Roberts, and J. White, "Educational Vulnerability Management Platforms: Capabilities and Limitations," Journal of Cybersecurity Education, vol. 8, no. 2, pp. 78-92, 2022.
[9] Apache Software Foundation, "CVE-2021-44228: Remote Code Execution in Log4j 2," Apache Security Advisory, Dec. 2021. [Online]. Available: https://logging.apache.org/log4j/2.x/security.html
[10] MITRE Corporation, "ATT&CK Framework for Enterprise," 2024. [Online]. Available: https://attack.mitre.org/
[11] T. Chen, L. Wang, and S. Liu, "Container Security in Cybersecurity Training Environments: Challenges and Solutions," in Proc. ACM Conference on Computer and Communications Security, 2023, pp. 1456-1467.
[12] K. Miller, R. Davis, and A. Johnson, "Assessment Methodologies in Cybersecurity Education: A Comprehensive Framework," IEEE Access, vol. 11, pp. 45678-45692, 2023.
[13] B. Taylor, M. Anderson, and P. Wilson, "Measuring Learning Effectiveness in Hands-on Cybersecurity Training Programs," Computers & Education, vol. 195, pp. 104-118, 2023.
[14] N. Zhang, Y. Li, and Q. Wang, "Scalable Cyber Range Architectures: Design Principles and Implementation Challenges," IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 892-905, 2023.
[15] H. Rodriguez, S. Kumar, and L. Thompson, "Open Source Cybersecurity Training Platforms: Community Development and Sustainability," ACM Computing Surveys, vol. 55, no. 8, article 167, 2023.