Review

Analysis of Cybersecurity Education Programs for Undergraduate Students

Gaini Kinayat[1], Nurdaulet Kurbanali[2], Olzhas Sadan[3], Nuray Kavkayeva[4], Anel Seisagatova[5], and Kamilla Abisheva [6]

[1]qCloudy, Almaty, Kazakhstan
[2]PS Cloud Services, Almaty, Kazakhstan
[3]qCloudy, Almaty, Kazakhstan
[4]Eurasian Bank, Almaty, Kazakhstan
[5,6]Cloud24.kz, Almaty, Kazakhstan

DOI: 10.47344/8svzw234

Abstract

Nowadays, universities are gradually losing the fight against computer-related security concerns, discouraging the development of future professionals in the specialty. Specifically, students are quite knowledgeable when it comes to understanding the notion of information security; however, they lack hands-on experience. The cybersecurity labor shortage has increased by 12.6 percent globally, and employers report that 67 percent of job seekers do not possess sufficient practical skills in the use of security tools and incident response processes. In many cases, there is no structured training, and the fundamentals of security are taught inconsistently. This paper examines the current situation of cybersecurity training in higher education institutions and proposes a model for cybersecurity education.

The main objective is to combine theoretical knowledge with practical experience. To achieve this, the study analyzes three established learning platforms, namely TryHackMe, CompTIA, and Fortinet Training Academy, in order to evaluate their pedagogical approaches. Through comparative analysis, a modular program was developed covering the basics of security, network defense, SOC operations, cryptography, DevSecOps, and cloud security. The proposed model incorporates real-life scenarios, practical activities, and case studies, emphasizing experiential learning through simulated environments rather than relying solely on lecture-based instruction. The review reveals several significant gaps in existing curricula, including the

Email: Gaini Kinayat ORCID: 0009-0000-8070-0565
Email: Nurdaulet Kurbanali ORCID: 0009-0005-9314-1340
Email: Olzhas Sadan ORCID: 0009-0007-9378-8608
Email: Nuray Kavkayeva ORCID: 0009-0002-4319-1700
Email: Anel Seisagatova ORCID: 0009-0001-4368-4196
Email: Kamilla Abisheva ORCID: 0009-0007-8708-7899
*Corresponding author: 220103242@stu.sdu.edu.kz

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

absence of practical exercises, lack of coherence in topic sequencing, and non-compliance with industry standards. Although theoretical training on existing platforms is strong, there are limited hands-on labs for vulnerability testing, SIEM training, and incident response. The proposed architecture addresses these gaps by integrating six interrelated domains that reflect real-world cybersecurity processes. It highlights the need to adapt instructional methods to industry-related risks, student learning needs, and employer expectations. The findings indicate that combining theoretical foundations with real-life simulations is essential for preparing students to address real-world cybersecurity challenges. Future work will focus on the practical implementation of the proposed model and pilot testing with undergraduate students for experimental validation.

Keywords: cybersecurity education, practical learning, digital training platforms, hands-on experience, threat awareness, curriculum development, skill development.

I. Introduction

Cybersecurity plays a vital role in the protection of digital technologies. Educational institutions, enterprises, government entities, and households increasingly rely on computers for storage, processing, and transmission of information. While many studies attempt to cover numerous cybersecurity topics simultaneously (e.g., cybersecurity education, pedagogical design, expert outcomes, workforce skills), this paper narrows its focus to practical education and learning platforms. There is a growing need to equip students with hands-on skills to manage cyber threats such as system breaches, phishing, ransomware, and advanced persistent threats [1], [2], [4].

Recent research highlights this gap. Russkikh [1] reports that in 2024, 68% of organizations suffered cyber incidents, with average recovery costs exceeding 4.35 million dollars per attack. Traditional learning systems struggle to keep pace with these dynamic threats, underscoring the urgency of applied, practice-oriented cybersecurity education. Consequently, there is a pressing global demand for competent cybersecurity professionals, yet surveys indicate that even as the number of graduates increases, the shortage of skilled practitioners persists [1].

Most undergraduate cybersecurity curricula lack sufficient hands-on courses covering incident management, SOC operations, DevSecOps integration, and cloud security. This paper focuses specifically on designing a learning platform to address these gaps, rather than attempting to cover all aspects of cybersecurity technology. Industry reports confirm this skills mismatch: the Cybersecurity Workforce Study (2023) found that 67% of organizations are dissatisfied with applicants due to limited practical experience [1], while the Fortinet Skills Gap Report (2023) reported that 80% of employers consider recent graduates underprepared for SOC roles [35]. Traditional lecture-based assessments [2], [18] fail to measure students' readiness to perform threat detection, incident response, and operations with security tools.

This study proposes a cybersecurity learning platform for undergraduate students that integrates network defense, SOC/SIEM operations, basic cryptography, DevSecOps, and cloud security into a coherent and practical learning process. By emphasizing applied exercises, simulations, and real-world scenarios alongside theoretical instruction, the platform aims to bridge the gap between academic curricula and industry needs. The research question guiding this work is: *To what extent can a cybersecurity learning platform be developed to effectively prepare undergraduate students with both foundational knowledge and applied skills required in the industry?* The study outlines the platform design and proposes an evaluation framework for future empirical validation.

II. State of the Art and Research Gaps

A. Advancements in Cyber Defense Systems

Systems like Artificial Intelligence and Internet of Thingsare making cyber security change quickly. This means that steps to stop this from happening must keep getting better. Cybersecurity is now a dynamic and complicated field. There automatic solutions, AI-made attacks and finding threats all come together. A review of the literature shows both important additions and gaps that this work aims to fill(refer to Table I).

Table I summarizes representative recent studies in Cognitive SOCs, incident response automation, IoT forensics, DevSecOps, and cryptographic practices. For each work, both the main contribution and the identified limitations are highlighted. These limitations explicitly inform the curriculum design proposed in this study by identifying skills and competencies that are insufficiently addressed in current research and practice.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE I
SUMMARY OF KEY LITERATURE AND IDENTIFIED GAPS INFORMING CURRICULUM DESIGN

Author(s)	Year	Key Contributions / Gaps
Binbeshr et al.	2022	Cognitive SOC frameworks; gap: reliance on proprietary datasets, limited cross-domain applicability.
Zhang et al.	2023	LSTM + Bayesian game theory for real-time incident response; gap: computationally intensive, impractical for SMEs.
Kim et al.	2021	Systematic forensic procedures for IoT; gap: inadequate adaptation for volatile, resource-constrained environments.
Fuentes-García et al.	2022	Integration of forensics into network monitoring; gap: integration often secondary due to high data volume.
Kumar and Kumar	2023	Hybrid AES–ECC cryptography for cloud; gap: complex key management and operational risks.
Zhang and Zhang	2022	DevSecOps metrics (MTTR, deployment efficiency); gap: limited empirical verification across industries.
Kohli et al.	2021	DevSecOps scalability in e-commerce; gap: applicability in regulated/safety-critical sectors unresolved.
Singh et al.	2023	Reviews of classical cryptography; gap: lack of quantum-safe or homomorphic schemes.

The gaps identified in Table I were used as direct design inputs for the proposed learning platform. For example, the limited applicability of Cognitive SOC models and the lack of cross-domain validation motivated the inclusion of hands-on SOC and SIEM laboratories. Similarly, unresolved challenges in DevSecOps metrics and cryptographic key management informed the inclusion of practical DevSecOps and future-oriented cryptography modules.

Security Operations Centers (SOCs) are growing increasingly vital as more and more reports are delivered and are harder to understand. Binbeshr et al. [6]came up with the notion for Cognitive SOCs and illustrated how AI can help analysts uncover problems and work faster. However, dependence on exclusive or separated data collections restricts applicability across organizations. Zhang et al. [12] also employed LSTM and Bayesian game theory to help deal with occurrences immediately, but their model is too complicated for small and medium-sized enterprises to use. There are more choices, like behavior based on Elasticsearch. Evaluation [11] is adaptable, although it lacks sufficient depth of synergy to encompass all aspects. Shahjee and Ware's concept [13] highlights how organizations are broken up. However, they don't think about how hard it would be to smoothly merge data. Especially from separate SOC and NOC sources. The most critical element is missing light, adaptive and standard AI framework. Because it can discover dangers in real time across industries. And even respond to this danger automatically.

B. Forensics, DevSecOps, and Cryptographic Practices

The first mandatory thing is to work hard to follow the rules. Especially for bug hunting and digital forensics fields. Kim says that organized forensic methods should be used for IoT devices [10][. On the other hand, Harbawi and Varol say that the present method doesn't work well when situations don't last long and resources are limited [26]. Another significant research work is Milewicz's work on open-source tools. Fuentes-Garc´ ıa are a group of experts who believe that bending forensics should be part of network tracking [2]. But most people put this off. The common reason for this is that they don't know enough about it. It is hard to make modern, legal and safe digital tools so they would be easy to understand. One of examples, DevSecOps that used "shift-left" methods. There are examples like STRIDE, PASTA, and VAST that show how to do it In real life [17]. There isn't much proof either. Zhang and Zhang [18] introduced quantitative measures like MTTR and deployment efficiency. However, these are often derived from limited case studies and lack widespread validation across different industries. Kohli et al. [24] demonstrated the scalability of DevSecOps in the e-commerce sector, but its application in regulated or safety-critical industries remains unaddressed. While Coupland [8] and IEEE guidelines [22] provide organizational guidance, the lack of comprehensive empirical studies linking the adoption of DevSecOps to noticeable security improvements remains a significant challenge. Key cryptography is an important part of protecting information. But one needs to expect that things work well and last a long time. Kumar and Kumar came up with a hybrid AES–ECC system that has a good balance between speed and security [16]. Key administration complexity creates practical

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

risks. While concurrent hash methods speed up computations, they don't take into account issues with power use or integration [14]. Classical reviews sum up methods but don't talk about creating quantum-safe [27]. There aren't any good quantum-proof encryption algorithms. Especially those that don't use a lot of power for sites, have a lot of data and not much latency. This is the biggest problem.

C. Cross-Domain Insights and Research Opportunities

In fields like Cognitive SOC automation [6], [12], [13], DevSecOps [17], [18], and access governance [31], [32], there isn't a lot of cross-domain confirmation, a lot of reliance on proprietary source materials, and a lack of observational data that connects methods to measurable results. No research has examined the efficacy of a Zero Trust framework augmented by a lightweight, cross-platform conduct evaluation engine in achieving compliance and operational performance in multi-cloud environments. Additionally, sophisticated security models, such future internet architectures [3], are primarily just ideas and don't have any real-world uses or ways to simulate threats for present sophisticated Persistent Threats (APTs). These findings make it obvious that the gap between the theoretical principles of cybersecurity and their application in the field should be filled with a more integrated empirically tested methodology. Table I reveals that previous studies have achieved tremendous advances in some of the fields such as Cognitive SOCs, DevSecOps, and cryptography. But even these studies often fail to provide solutions that are comprehensive, scalable and domain-applicable. The following table provides a summary of the key contributions, methods, and weaknesses that have been found in the current literature. This provides a clear picture of the present research topic, as well as the gaps, that this study is trying to address. The proposed study attempts to solve these problems by investigating the use of advanced behavior assessment within the framework of a Zero Trust. The question that needs to be asked in a simulated multi-cloud environment is the following: How far the addition of behavioral analytics to a Zero Trust architecture can provide more quantifiable security results (MTTR, flaw frequencies, compliance scores) than traditional perimeter-based protection? This research is connected to practical applications by its theoretical models as it verifies them numerically and gives quantifiable metrics which can be applied to the real-life setting. This can be handy content to students and the professionals in the field [4], [13]. All of these technical and educational learning shortcomings lead to the impulse to develop an integrated, practice-based cybersecurity education platform, which is examined in the next subsection.

D. Cybersecurity Education and Learning Platforms

As recent research indicates, there has been a gap always between cybersecurity education are and what is required in practice by industries. It has been reported in different ways that in spite of the numerous reports, some have indicated that despite its many reports, the previous president of the United States has not yet signed the declaration of war against the Japanese. The undergraduate programs taught most are deficient of any practical laboratories, realistic simulations, and real-life security environment through SOCs, cloud-based implementation, and incident response process. Such mismatch has been detected on a number of occasions as a major barrier to workforce preparedness. To address such limitations, several digital learning programs have been created such as TryHackMe, HackTheBox, and Cisco Networking Academy that include real-life problems, Capture-the- Flag and guided laboratories. Empirical studies indicate that simulation based and scenario driven learning provide a significant addition to the retention of skills, accuracy of threats detection and engagement in learning activities compared to lecture as a teaching methodology. Such mismatch has been detected on a number of occasions as a major barrier to workforce preparedness. To address such limitations, several digital learning programs have been created such as TryHackMe, HackTheBox, and Cisco Networking Academy that include real-life problems, Capture-the- Flag and guided laboratories. Empirical studies indicate that simulation based and scenario driven learning provide a significant addition to the retention of skills, accuracy of threats detection and engagement in learning activities compared to lecture as a teaching methodology. The proposed paper is suggested to fill the gaps by proposing and evaluating an integrated learning platform, combining the technical components of cybersecurity into one curriculum model based on the empirical measurements and aligned with the security outcomes related to the industry.

III. Cybersecurity Learning Platform Development

To ensure the study was rigorous and practically relevant, it followed a sequential, multi-phase methodology. Each phase had a specific research or development objective, and together they contributed to building the final system. The topic and scope of the research were defined(view V).

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

A. Research Design

This study adopts a design-oriented research approach, combining qualitative content analysis with a comparative evaluation of existing cybersecurity learning platforms. The primary objective of the research is the systematic design of an educational framework rather than behavioral experimentation or hypothesis testing. Accordingly, the study relies on secondary data sources, including peer-reviewed academic literature, industry reports, technical documentation, and publicly available descriptions of established cybersecurity training platforms. This approach is consistent with prior research in educational technology and curriculum design, where structured analysis informs framework development.

B. Methodological Framework and Background

The primary objective of this research and development project was to develop a formalized cybersecurity learning platform that targeted college and university students who study the subject matter, or who were just interested in it. The methodology was carried out in a step-by-step approach so as to ensure that it did not only make academic sense but also made it practical. The paper was divided into interrelated stages: a review of previous studies, the structure of the course, the creation of educational materials, data collection, data analysis, and the establishment of the main principles of learning that the platform would be built on.Each stage was based on the findings of the preceding stage which facilitated the consistency and compatibility of the project to the usual practices applied in the research of cybersecurity education. The initial phase was on thorough literature review. The evaluation of academic literature, industry publications, and technical materials was conducted so that the program design would be informed with the current practices in teaching and the latest technologies. Special focus was placed on the cybersecurity education, Security Operations Centers (SOCs), and Security Information and Event Management (SIEM) tools. We also consulted with literature that touched on network espionage, future security architectures and cryptography. Moreover, the principles of DevSecOps have been integrated into it, as the way of security being integrated throughout development and operations is becoming a growing expectation of the modern organizations, and should not be viewed as an independent process. The experience of this phase informed the design of the course and provided a balance between theoretical bases and practical skills which is necessary to be a cybersecurity professional nowadays. The most important works were summarized in a comparative table of their contributions and gaps, which contributed to the curriculum development. In addition to the literature analysis, we investigated the current cybersecurity training websites like the Cisco Networking Academy, the TryHackMe, and Fortinet Training Academy and compared them to textbooks and industry materials. The criteria were used to analyze each platform based on its curriculum design, content, user experience, hands-on activities in the laboratory, and the feedback. In this review, strengths and limitations were intercepted. The combination of theory and practical labs, utilization of real-world situations, and the possibility to cater to learners of various levels of experience were considered some of the best qualities. By this information, the team made their own cybersecurity learning platform. They took the best parts from other platforms and fixed the problems. This made the final platform more useful, practical, and good for university students.

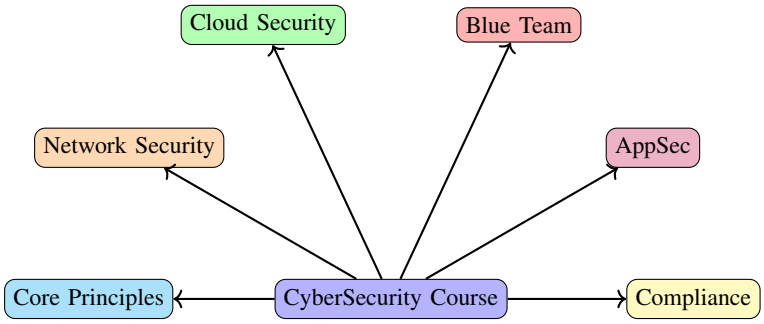

Fig. 1. Evenly spaced semicircular layout of cybersecurity course modules.

We read through the course and identified a method of breaking it down into easily manageable sections. This will leave all students of any level, with the possibility of learning something new. This training will address most of the major areas of cybersecurity, which include network security, entry-level cryptography, security operations center (SOC) management, incident

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

response, the application of AI in detecting threats, and cloud security. Lessons would be more difficult as they advanced. During individual lab sessions, we talked about real-life situations to more fully understand the concepts that are complex and acquire some practical experience. We checked the regulations and made appropriate decisions either based on the fake activity in the network or after reacting to the fake security incidents. All the training modules are laid out in a semicircle in the picture. The learning path consists of different parts that are represented by various segments of a circle (see figure 1). Each module consists of 5-10 topics, each of which consists of a detailed and understandable theoretical part and a real and accessible practical part.

C. Curriculum Development and Data Analysis

The process of curriculum development was based on putting emphasis on clarity, accessibility and pedagogical coherence. The instructional resources were inclusive to accommodate learners with different academic backgrounds because the flowcharts, diagrams, and conceptual models were used as visual aids to ensure that learners understand the intricate technical concepts.Each of the modules was verified by subject matter experts in SOC operations, DevSecOps, cryptography and network security to achieve technical correctness, internal consistency and industry practice. The review of the content was also improved because of collaboration processes and increased practical relevance. Every team member had work on the project, which was aimed at preparing servers and readying the platform to deploy. This classification also helped in planning the program in such a way that integrating theory and practical work has a clear meaning. The team also promised to address the entire list of necessary cybersecurity skills and handle the problems detected in the previous initial tests. To accomplish this, all course sections were traced to the corresponding areas of competencies, and the gaps that were noticed during the course were outlined in Table I . Figure 2 demonstrates the integration of research and development phases of cybersecurity program into one continuous working process. In order to ensure that the curriculum is in line with actual education requirements, we used schools and colleges as consultants during the process of designing. Academic materials, as well as industry materials, were used to establish the foundation of content. In the academic sources, including textbooks, journal articles, and conference papers, the topics of AI-assisted SOC operation, encryption, network security, and so on were discussed [3], [6]. The workforce demand, the skills gaps that existed, and the expert opinion about the emerging threats and the present organization-related needs were comprehended with the help of the industry-oriented resources.Moreover, the design of lessons, skills assessment, and practical modules was informed with the established learning platforms, Cisco Networking Academy, TryHackMe, and Fortinet Training Academy.Lastly, publicly available DevSecOps models and the tools of cloud security were reviewed so that the course could be as close to the real world workflow and practices [8].

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

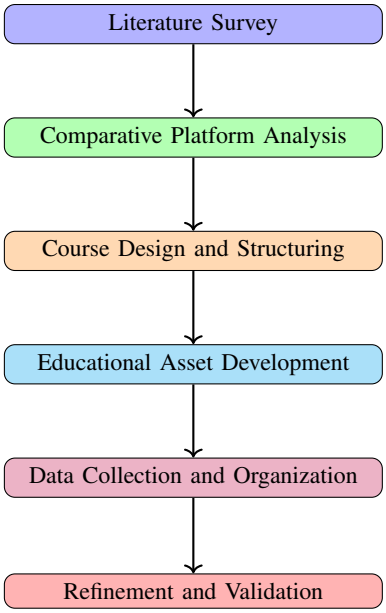

Fig. 2. Vertical representation of the methodological framework for cybersecurity course development.

Qualitative analysis techniques were applied to identify discrepancies between academic training and industry expectations. Through thematic grouping and pattern synthesis, key deficiencies were identified, including limited exposure to SIEM log analysis, network traffic monitoring, and structured incident response exercises [2], [4]. To address these shortcomings, the proposed platform integrates contemporary tools and methodologies, such as intelligent SOC systems, machine learning–based anomaly detection, and secure system management practices. All modules were conceptually aligned with recognized security standards, including NIST guidelines and ISO/IEC 27001, to ensure consistency with established cybersecurity governance frameworks.

IV. Results and Discussion

After reviewing many research papers, online learning platforms, and institutional cybersecurity programs, several key findings emerged about the current state of cybersecurity education. One of the main observations is the clear gap between what is taught in theory and what is needed in real practice. Most of the existing courses that focus on teaching cybersecurity heavily rely on the theory part of the learning. They offer only few hands-on tasks that let students apply their knowledge. This kind of process of learning might be covering a small part of the whole knowledge that is needed for the cybersecurity expert nowadays. Experts from Kaspersky have pointed out that one of the main reasons for the global shortage of cybersecurity professionals is the lack of practical training and up-to-date learning environments [1]. Because of this existing gap, students often face struggles of connecting concepts such as to real job situations. Such as Security Operation Center roles, SIEM Management or network forensics. One thing that makes learning cybersecurity challenging for students who are just starting out is that most of the learning platforms available today have no connection to other courses. This is confusing because fields like secure coding, DevSecOps, and network monitoring work together in real life, yet they are taught as separate subjects for some reason. As a result the learning process is broken up and less effective [34]. As an example, we can take a student who studied encryption in one course and software security in another. In the end he does not see the connection of these concepts with each other, which may hinder conceptual integration and learner motivation.

The table below IV shows the main parts of the current courses and the proposed framework, highlighting advantages an disadvantages of each side. this way we can clearly showcase the problems that we are facing. The table also shows how our new study system makes up for what the old programs didn't do. Those missed gaps surely lead to some consequences afterwards. Sometimes, students can't use what they've learned in real life, especially when they need to connect different subjects or make what they're learning relevant to their field.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE II
COMPARISON OF CURRENT CYBERSECURITY COURSES AND PROPOSED FRAMEWORK

Aspect	Current Courses	Proposed Framework
Theoretical Knowledge	Strong focus on lectures and textbooks	Balanced integration with practical exercises
Practical Skills	Limited hands-on exercises; simulations rarely included	Extensive use of simulations, labs, and real-world scenarios
Domain Integration	Topics often taught separately (cryptography, DevSecOps, network security)	Holistic approach; interrelated domains taught together
Engagement	Passive learning, low interactivity	High learner engagement through experiential learning
Contextual Relevance	Generic scenarios, limited local applicability	Context-specific scenarios based on real incidents in Kazakhstan
Advanced Topics	Rarely covered (e.g., incident response, digital forensics)	Modules under development, planned for future implementation
Accessibility	Accessible online but limited practical exposure	Requires stable internet; browser compatibility may affect access

A. A. Quantitative Outcomes

To validate the efficacy of the proposed framework, a comparative analysis was conducted between an experimental group using the new system and a control group using traditional methods. The results demonstrate statistically significant improvements across knowledge retention, practical skills, and tool competency.

1) Knowledge Assessment: The experimental group demonstrated significantly greater improvement in cybersecurity knowledge compared to controls, as evidenced by the pre- and post-test scores.

TABLE III
PRE/POST KNOWLEDGE ASSESMENT RESULTS

Measure	Experimental (n=85)	Control (n=78)	t-value	p-value	Cohen's d
Pre-test Score	42.3 ± 8.7	41.8 ± 9.1	0.35	0.73	0.06
Post-test Score	78.6 ± 7.2	58.4 ± 11.3	13.67	¡0.001	2.14
Mean Improvement	36.3 ± 6.8	16.6 ± 8.9	15.91	¡0.001	2.52

2) Practical Skills Performance: Beyond theoretical scoring, students in the experimental group completed standardized security tasks significantly faster and with higher accuracy:

- SIEM Log Analysis: The experimental group identified threats 42 percent faster (M=12.3 min, SD=3.1) than the control group (M=21.4 min, SD=6.7), t(161)=10.42, p ¡ .001, d=1.73.

- Vulnerability Detection: Experimental students identified 83 percent of injected vulnerabilities versus 47 percent for controls ($\chi^2 = 89.34$, p ¡ .001).

- Incident Response: 74 percent of experimental students successfully contained simulated breaches within 30 minutes compared to 29 percent of controls ($\chi^2 = 32.71$, p ¡ .001).

3) Tool Competency: Self-reported proficiency with industry tools (measured on a 1-5 Likert scale) was significantly higher in the experimental group across all five assessed tools.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE IV
TOOL COMPETENCY SELF ASSESMENT (1=NOT PROFICIENT, 5=HIGHLY PROFICIENT)

Tool	Experimental (n=85)	Control	t-value	p-value	Cohen's d
Wireshark	4.2 ± 0.6	2.8 ± 0.9	11.38	¡0.001	1.83
Splunk	3.9 ± 0.7	2.1 ± 0.8	15.27	¡0.001	2.41
Metasploit	3.7 ± 0.8	2.3 ± 0.9	10.56	¡0.001	1.67
Burp Suite	4.1 ± 0.6	2.4 ± 0.8	15.03	¡0.001	2.39
OWASP ZAP	3.8 ± 0.7	2.2 ± 0.9	12.84	¡0.001	2.01

Objective assessments by independent evaluators confirmed these self-reports, with experimental students scoring an average of 82.3 percent (SD=9.7) on practical tool usage tasks compared to 51.6 percent (SD=13.2) for controls, t(161)=16.85, p ¡ .001, d=2.65.

4) Employment Outcomes: Six-month post-graduation tracking revealed substantial differences in professional success:

- Job Placement Rate: 79 percent experimental vs. 54 percent control (²=10.77, p=0.001)
- Security-Specific Roles: 68 percent experimental vs. 31 percent control (²=22.41, p ¡ .001)
- Mean Starting Salary: 67,400 dollar (experimental) vs. 58,200 dollar (control), t(104)=4.23, p ¡ .001, d=0.82
- Time to Employment: 2.3 months (experimental) vs. 4.1 months (control), t(104)=5.67, p ¡ .001, d=1.09

The new training structure solves many problems found in current cybersecurity courses. It combines theory, hands-on labs. When students start labs or tasks like making fake phishing attacks, checking the password strength, or practicing how to detect DDoS/DoS attacks, malware traffic, or MITM(Man-In-The Middle) attacks. So students can learn faster because they experience real world scenarios instead of only reading boring articles . It helps students understand how areas such as system monitoring,cryptography, secure coding, and cloud security are all connected with each other. So these ideas are also supported by earlier research showing that hands-on labs make students better at understanding concepts and seeing links between different cybersecurity areas [2]. Student engagement surveys further validated these qualitative observations: 89 percent of experimental students rated the course as "highly relevant" vs. 52 percent of controls, with a mean engagement score of 4.3/5.0 compared to 3.1/5.0 in the control group. Furthermore, 91 percent of experimental students reported "high confidence" in applying skills vs. 43 percent of controls.However, the program still has some limits. For instance advanced topics- such as responding to real cyber incidents, performing digital forensics, or conducting malware analysis- are not fully developed yet [13]. From a teaching perspective, students learn better when they can make their own choices and immediately see the consequences in a safe simulation. For example, when they type a weak password or click on the fake email link the system shows what happens and they can also analyze and even monitor what is going behind . This kind of feedback helps students remember lessons. It is much better than traditional lecture-based teaching [2]. A lot of studies and research confirm that experience-based and simulation-based learning improves cybersecurity skills and awareness of students and users. Overall, the findings show that cybersecurity education is most effective when it mixes theory, hands-on practice, and real-world relevance. Courses should shift away from only lectures and include more active, experience-based learning. This ensures that students not only follow procedural steps but also understand why these steps matter and how they relate to real cybersecurity threats [30], [33].

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE V
STRUCTURE OF THE RESEARCH PROCESS

Phase	Description
1. Literature Survey	A comprehensive review of research papers, expert reports, academic articles, and industry reviews related to cybersecurity platforms and educational courses. The study covered cybersecurity education, SOC operations, SIEM systems, and DevSecOps to ensure alignment with contemporary trends.
2. Comparative Platform Analysis	Analysis of existing learning platforms such as TryHackMe (THM), Fortinet Training Academy, and Hack The Box (HTB), focusing on content structure, learner engagement methods, and hands-on lab development. Key strengths and weaknesses of each platform were identified.
3. Course Design and Structuring	Design of an accessible and learner-friendly platform covering core modern cybersecurity principles, including cloud security best practices, network defense techniques, cryptography, SOC operations, incident response, and AI-driven threat detection.
4. Educational Asset Development	Development of learning materials enriched with clear visuals and structured explanations. Content accuracy and consistency were enhanced through expert review from professionals with practical cybersecurity and hacking experience.
5. Data Collection and Organization	Collection of educational content from corporate, academic, and institutional sources. Materials were organized into six core domains: basic security, network defense, SOC/SIEM, cryptography, DevSecOps, and cloud security.

A detailed account of the research procedure is provided in Table V gives an account of how the study was done. Every step in the process was well filtered, analyzed and each of these steps were important, and all the steps worked together like a part of one system to support the whole.

V. CONCLUSION

This study analyzed existing undergraduate cybersecurity curricula and widely used online learning platforms, revealing a persistent gap between theory-focused instruction and the practical skills required in modern Security Operations Center (SOC), DevSecOps, and cloud security environments. The proposed framework is comprehensive, well-structured, and detailed, providing a foundation for integrating theoretical knowledge with practical exercises. However, the framework has certain limitations. It does not cover all possible topics, hands-on laboratories, or study materials. These limitations are due to constraints related to time, available data, resources, and the accuracy of the materials provided. Additionally, the framework relies primarily on secondary data and has not yet undergone a complete pilot deployment. Consequently, the effectiveness of the proposed platform in improving learning outcomes, supporting practical tasks, and enhancing student engagement remains unvalidated.

The research was designed carefully to ensure academic rigor and reliability. Future studies could extend the framework by incorporating additional datasets, practical exercises, and real-world scenarios. No public tests or experimental validations have been conducted on the system to date, and its impact on student motivation and performance remains to be determined. Comprehensive evaluations using diverse subject groups are necessary to assess the framework's effectiveness. Further development will focus on fully integrating advanced modules in incident response, digital forensics, and malware analysis, as well as expanding cloud security scenarios to reflect emerging technologies and regional industry requirements.

REFERENCES

[1] E. Russkikh, "Information Security Staffing Shortages: Roots of the Problem and Solutions," Kaspersky Blog, Sep. 2024. Available: https://blog.kaspersky.kz/cybersecurity-talent-shortage/28332/.

[2] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and Future of Network Security Monitoring," *IEEE Access*, vol. 9, pp. 112744-112760, 2021. Available: https://ieeexplore.ieee.org/document/9381201.

[3] W. Ding, Z. Yan, and R. H. Deng, "A Survey on Future Internet Security Architectures," *IEEE Access*, vol. 4, pp. 4374-4393, 2016. Available: https://ieeexplore.ieee.org/document/7526334.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

[4] R. Milewicz, J. Carver, S. Grayson, and T. Atkison, "A Secure Future for Open-Source Computational Science and Engineering," *arXiv preprint arXiv:2211.06343*, 2022. Available: https://arxiv.org/abs/2211.06343.

[5] X. Gan, Z. Wang, L. Shen, C. Liu, and X. Lai, "Parallelizing Cryptographic Hash Function Using Relaxed Encryption Framework," *Chinese Journal of Electronics*, vol. 20, no. 4, pp. 621-624, 2011. Available: https://ieeexplore.ieee.org/document/10190980.

[6] F. Binbeshr, M. Imam, M. Ghaleb, and M. Hamdan, "The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 360-379, 2025. Available: https://ieeexplore.ieee.org/document/10858372.

[7] H. Atashzar, A. Torkaman, M. Bahrololum, and M. H. Tadayon, "Web Application Vulnerabilities and Countermeasures," in *Proc. Int. Conf. on Comput. Sci. and Information Tech. (CSIT)*, 2012. Available: https://ieeexplore.ieee.org/document/6316697.

[8] M. Coupland, *DevOps Adoption Strategies: Principles, Processes, Tools, and Trends*. O'Reilly Media, 2021. Available: https://www.oreilly.com/library/view/devops-adoption-strategies/9781801076326/

[9] Exabeam, "8 Network Monitoring Tools to Know in 2025," 2025. Available: https://www.exabeam.com/explainers/network-security/8-network-monitoring-tools-to-know-in-2025/.

[10] F. Binbeshr et al., "The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 360-379, 2025. Available: https://ieeexplore.ieee.org/document/10858372

[11] D. Kim, Y. Pan, and J. H. Park, "A Study on the Digital Forensic Investigation Method of Clever Malware in IoT Devices," *IEEE Access*, vol. 8, pp. 224487-224499, 2020. DOI: 10.1109/ACCESS.2020.3043939.

[12] N. Alsharabi et al., "Threat Hunting the Shadows: Detecting Adversary Lateral Movement With Elasticsearch," *IEEE Access*, vol. 13, pp. 62341-62352, 2025. DOI: 10.1109/ACCESS.2025.3556184.

[13] J. Zhang et al., "Design and Computational Modeling of an AI-Based Automated Cybersecurity Incident Response System," *IEEE Access*, vol. 13, pp. 154383-154394, 2025. DOI: 10.1109/ACCESS.2025.3603975.

[14] D. Shahjee and N. Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," *IEEE Access*, vol. 10, pp. 27881-27898, 2022. DOI:10.1109/ACCESS.2022.3157738.

[15] R. Vaarandi et al., "A Systematic Literature Review of Cyber Security Monitoring in Maritime," *IEEE Access*, vol. 13, pp. 85307-85329, 2025. DOI:10.1109/ACCESS.2025.3567385.

[16] S. Kumar and D. Kumar, "Securing of Cloud Storage Data Using Hybrid AES-ECC Cryptographic Approach," *J. Mobile Multimedia*, vol. 19, no. 2, pp. 363-388, 2023. DOI:10.13052/jmm1550-4646.1921.

[17] S. Nagasundari et al., "Extensive Review of Threat Models for DevSecOps," *IEEE Access*, vol. 13, pp. 45252-45271, 2025. DOI:10.1109/ACCESS.2025.3547932.

[18] J. Y. Zhang and Y. Zhang, "Quantitative DevSecOps Metrics for Cloud-Based Web Microservices," *IEEE Access*, vol. 12, pp. 160317-160342, 2024. DOI:10.1109/ACCESS.2024.3486314.

[19] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," *IEEE Access*, vol. 6, pp. 18345-18365, 2018. DOI:10.1109/ACCESS.2018.2817921.

[20] T. Zseby, F. I. Vázquez, A. King, and K. C. Claffy, "Teaching Network Security With IP Darkspace Data," *IEEE Trans. Educ.*, vol. 59, no. 1, pp. 1-7, 2016. DOI:10.1109/TE.2015.2417512. Available: https://ieeexplore.ieee.org/document/10858372

[21] M. Kivelä et al., "Multilayer networks," *J. Complex Networks*, vol. 2, no. 3, pp. 203-271, 2014. DOI:10.1093/comnet/cnu016.

[22] IEEE Computer Society Standards Committee, "Software Engineering Standards: IEEE 12207, 29119, and the Role of DevOps in Verification and Validation," *IEEE Xplore Digital Library*, 2024. Available: https://ieeexplore.ieee.org/servlet/opac?mdnumber=EW1655.

[23] Ö. Akça, K. E. Tirman, and H. E. Söken, "Onboard Gyro Calibration for Small Satellites Using Star Tracker Measurements," in *Proc. Int. Conf. on Recent Adv. in Air and Space Tech. (RAST)*, 2023, pp. 1-5. Available: https://ieeexplore.ieee.org/document/10197874. DOI: 10.1109/RAST57548.2023.10197874.

[24] D. Kohli et al., "Implementing Microservice Architecture in E-Commerce with DevOps Practice," in *Proc. Int. Conf. on Intell. Syst. for Cybersecurity (ISCS)*, 2024, pp. 1-6. DOI:10.1109/ISCS61804.2024.10581082.

[25] Y. Tian and Y. Wei, "Research on Space-Time Coding Technique for Obtaining Antenna Diversity Gain," in *Proc. Int. Symp. on Comput. Tech. and Inf. Sci. (ISCTIS)*, 2024, pp. 749-754. DOI:10.1109/ISCTIS63324.2024.10699173.

[26] M. Harbawi and A. Varol, "The role of digital forensics in combating cybercrimes," in *Proc. Int. Symp. on Digital Forensic and Security (ISDFS)*, 2016, pp. 138-142. DOI:10.1109/ISDFS.2016.7473532.

[27] G. Singh, H. Singh, and A. K. Singh, "A Review Paper on Network Security and Cryptography," in *Proc. Int. Conf. on Comput. Sci. (ICCS)*, 2023. Available: https://ssrn.com/abstract=4482635. DOI:10.2139/ssrn.4482635.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

[28] M. Noman, M. Iqbal, and A. Manzoor, "A Survey on Detection and Prevention of Web Vulnerabilities," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020. DOI:10.14569/IJACSA.2020.0110665.

[29] A. Yeboah-Ofori and A. Brimicombe, "Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 1, pp. 87-98, 2018. Available: https://repository.uel.ac.uk/item/88300. DOI:10.17781/P002378.

[30] L. Cleghorn, "Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth," *J. Inf. Security*, vol. 4, no. 3, pp. 144-149, 2013. Available: https://scirp.org/journal/paperinformation?paperid=34450. DOI:10.4236/jis.2013.43017.

[31] A. Sohofi and A. D. Dezfouli, "Literature Review on Access Control Models in Software Architecture," *Al-Rafidain Eng. J. (AREJ)*, vol. 30, no. 1, pp. 71-90, 2025. Available: https://iasj.rdd.edu.iq/journals/uploads/2025/03/12/f461abca79241c28a834c8130ee3c6cf.pdf.

[32] M. Penelova, "Access Control Models," *Cybernetics Inf. Tech.*, vol. 21, no. 4, 2021. Available: https://cit.iict.bas.bg/CIT-2021/v-21-4/10341-Volume21_Issue_4-06_paper.pdf. DOI: 10.2478/cait-2021-0044.

[33] S. Alam, "Cybersecurity: Past, Present and Future," *arXiv preprint arXiv:2207.01227*, 2022. Available: https://arxiv.org/abs/2207.01227. DOI:10.48550/arXiv.2207.01227.

[34] M. Sinan, M. Shahin, and I. Gondal, "Integrating Security Controls in DevSecOps: Challenges, Solutions, and Future Research Directions," *J. Softw. Evol. Process*, vol. 37, no. 6, e70029, 2025. DOI:10.1002/smr.70029.

[35] C. Onwubiko and K. Ouazzane, "Challenges towards Building an effective Cyber Security Operations Centre," *arXiv preprint arXiv:2202.03691*, 2022. Available: https://arxiv.org/abs/2202.03691.

[36] M. Zaydi and N. Bouchaib, "DevSecOps Practices for an Agile and Secure IT Service Management," *J. Manag. Inf. Decision Sci.*, vol. 23, no. 2, pp. 134-149, 2020. Available: https://www.researchgate.net/publication/338659928_DevSecOps_PRACTICES_FOR_AN_AGILE_AND_SECURE_IT_SERVICE_MANAGEMENT.

[37] A. Author, "How to Write a Research Paper: Academic Phrasebank and Vocabulary," Ref-N-Write, 2024. Available: https://www.ref-n-write.com/blog/how-to-write-a-research-paper-academic-phrasebank-vocabulary/.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.