**Edelweiss Applied Science and Technology**
*ISSN: 2576-8484*
*Vol. 9, No. 6, 2203-2212*
*2025*
*Publisher: Learning Gate*
*DOI: 10.55214/25768484.v9i6.8336*


# A virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students

Krommavut Nongnuch[1*], Pinyaphat Tasatanattakool[1], Suthin Kasetrattanachai[1], Pallop Piriyasurawong[2]
[1]Rajamangala University of Technology Suvarnabhumi, Ayutthaya, Thailand; krommavut.n@rmutsb.ac.th (K.N.).
[2]King Mongkut's University of Technology North Bangkok, Bangkok, Thailand.

**Abstract:** This research aims to improve and evaluate a virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students. Conducting artificial research, designing, and assessing the feasibility of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students through a process according to a conceptual framework model divided into six steps: 1) Preparation: Student HE is a group of higher education students. Virtual Team is building a team for learning and dividing educational duties as planned. Network Simulator is a program for educational use offline or online. 2) Studying the incidents of cyber threats, narratives, missions, and purposes within the team to identify conditions, skills, knowledge, and learning styles. 3) Pre-test assessment. 4) Studying how to prevent cyber threats from previous cyber threat incidents—learning how to act according to the teamwork plan to improve competency (KSA) while measuring team performance. 5) Post-test assessment. 6) Applying the results to improve cyber threat incidents, narratives, missions, and purposes. The evaluation results of the model's feasibility from experts found that the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students is at an excellent level. The model can be incorporated into the coursework of higher education students to improve cybersecurity competency.

***Keywords:*** *Cybersecurity competency, Higher education, Network simulators, Virtual team collaboration.*

## 1. Introduction

Teamwork is an essential skill for higher education students. Skills in this field are necessary to prepare for work in the digital industry. Therefore, students should be trained or accustomed to accessible skills. The computer science department should significantly consider the higher demand of students regarding their abilities in a team environment and combining a broad range of computer fields. Teamwork while studying a computer science and engineering course positively impacts teamwork and assigning responsibilities. Team learning allows students to understand and implement better, which enhances teamwork skills [1].

Teamwork involves several critical aspects, one of which is cybersecurity. The limitation of team members is working together. Recognizing each other's knowledge, skills, and abilities can help enhance the strengths of each member, leading to improved academic teaching performance [2]. Studying cybersecurity has many new challenges and continuous efforts to meet the demands necessary for fieldwork [3]. The primary reason for the challenges mentioned above is the need for cybersecurity personnel who are better equipped to deal with emerging threats and combat cybercriminals, with an emphasis on competency as per the International Information System Security Certification Consortium. The current market demand for cybersecurity personnel requires a 145% increase in their numbers. At the same time, the number of cyber threat incidents is also increasing steadily and severely


**History:** Received: 9 April 2025; Revised: 9 June 2025; Accepted: 12 June 2025; Published: 24 June 2025
* Correspondence: krommavut.n@rmutsb.ac.th

[4] affecting the global economy and national security worldwide [5]. In this sense, higher education students are taught a learning approach to how to manage emerging cyber threats from previous incidents. This approach is an anchor for studying cybersecurity as it is an effective academic instrument. Nevertheless, learning and training in cybersecurity is a new approach yet to be studied [6] which still needs standard designs and conventional methods.

From the justification mentioned above, our research team has designed a model and an architectural approach for skills training in cybersecurity from previous cyber threat incidents to boost the efficiency in studying cybersecurity as a virtual team collaboration model using network simulators, emphasizing achieving improved learning of higher education students.

Objectives to study the conceptual framework of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students. Develop the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students. Evaluate the feasibility of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

Research Hypothesis feasibility evaluation results of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students is excellent.

Research Scope the demographic and subjects are qualified experts: two experts on virtual team collaboration, two experts on network simulators, and three experts on cybersecurity competency for higher education students. There are seven experts with a minimum of a 5-year of experience in their expertise to evaluate the designed learning model by purposive sampling.

Research Variables independent variable: The virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students. dependent variable: Feasibility evaluation of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students by experts.

## 2. Literature Reviews

### *2.1. Virtual Team Collaboration*

Collaboration through a medium, the fundamental teamwork principles, or even the coexistence of people in society or any organization enhances work efficiency by improving communication in virtual collaboration.

The generation of groups is one of the essential processes in team learning. The goal is to propose an approach based on a genetic algorithm to obtain groups between homogeneous and different internally. The main feature of the mentioned approach is to aid in determining the attributes of students as much as required [3].

After studying four pieces of research [2] it was found that collaborations were reported. Our team has been tasked with participating in international collaborations and have a strong understanding of team responsibility. We treat all opinions equally and possess awareness, intuition, and insight in this field. Other abilities, such as cultural skills, communication, and self-management, are categorized as part of the collaboration skill set but incorporated into the relevant domains mentioned earlier. Discussions on trust between individuals are the primary condition most mentioned for online success in collaborations [6].

Application-oriented teaching that combines the learning of small and large groups by integration of many small groups into large group settings is more frequently applied with suitable technology for the task or communication.

Choosing unsuitable instruments for the work would cause inconvenience rather than convenience. Thus, communication through words such as emails, messages, or bulletin boards, these channels are more appropriate for one-way communication, i.e., informing news and work plans, sharing ideas, or simple data collection. Whereas communication channels through websites or video conferences focus on two-way communication, this channel is ideal for joint problem-solving or negotiations. Accordingly, the more complicated the communication, the more private the communication instrument should be.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

*2.2. Network Simulators*

Simulation of the network functionality and network instruments to enhance the learning efficiency of the network, able to detect network behavior, and understand computer communication. The Intelligent Training Exercise Environment (i-tee) is a platform designed for fully automated cyber security contests. It includes several key elements, such as automated attacks, automatic scoring using a scoreboard, and background data volume generation [7].

High-accuracy network behavior can be caught when the node is adjusted to thousands of nodes using an error model. The bit error probability for the TOSSIM network remains simple and efficient but is expressed enough to capture a variety of network responses.

The framework of COFELET presents [8] the main elements that need to be considered in earnestly designing cybersecurity. Games accompanied by the interconnections of these elements in the game structure are the crucial concept of COFELET. The framework is work that composes of actions that are geared towards the fulfillment of the target game. The sequence that can be implemented is explained in Scenario Execution Flows (SEFs). SEFs were suggested to be defined by comparing them with attacking patterns, such as those outlined in CAPEC. The objectives of learning the educational environment and learning strategies are to facilitate elemental analysis in education and the intense gameplay of cybersecurity games and to connect these elements to the overall learning objectives of the game. The COFELET framework is consistent with the Activity Theory Model for the Game (ATMSG) and the Learning Mechanic-Game Mechanic (LMGM) model extensions

*2.3. Cybersecurity Competency*

Academic scholars and many experts can conclude that competency means knowledge, ability, and mindset to perform duties and gain efficiency successfully. Types of competencies stated that competency could be separated into three main types, which are, Core Competency means the primary ability that everyone is expected to have goals, visions, and successful missions. Overall, a core competency that can be performed continuously with other people. Managerial Competency means the capability to manage work, which is expected from employees and distinguished according to the level of the job position. In the case of the same job position, managerial competency is expected of each party, e.g., department managers disregarding the department all require competency in strategic visions, work planning, management, transformation, and network building. Determination of managerial competency is determined by the primary duties and responsibilities that are in common according to the level of the job position, and the number of rules of managerial competency should be reasonable. Function competency means the capability in specific tasks that vary in different departments. Determination of function competency depends on the job description by considering what each position expects of knowledge, skills, and individual characteristics in particular areas. These capabilities would affect the successful execution of the assigned work by the supervisor by estimating the success of the work from key performance indicators. Therefore, the number of function competencies have their uniqueness concerning the department. Generally, there are between 5-7 rules. Moreover, function competency can be further categorized into two sub-categories which are (1) Common Function Competency is the work capability in everyday tasks of other job positions in other departments, and (2) Specific Function Competency is the work capability in specific technical skills that requires expertise and time to learn and practice.

Cybersecurity means the process or all actions required to minimize risks and damages to the system that could impact information safety in all formats. This includes the security of the systems and networks used for storage, access, processing, and distributing data as well as waring and preventing crimes, attacks, espionage, and various mistakes, which risks could include things such as a breach of personal data protection and work disturbances.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

*2.4. Cybersecurity Competency*

Two major principles of higher education are academic freedom and open-mindedness. Encyclopedia Britannica described academic freedom as "Freedom of teachers and students in teaching, studying, seeking knowledge and researching in the absence of unreasonable interferences and restrictions from the law, institute regulations or social pressure." At the same time, open-mindedness is overly explained as a comprehensive concept or philosophy emphasizing transparency and collaboration [9]. Namely, open-mindedness means "Accessibility of knowledge, technology, and other resources with operational transparency, organizational structure permeability, and harmony." In practical collaboration [10] researchers are given intellectual freedom without the constraints of short-term deadlines typical in industry partnerships. The availability of funding and resources constrains the freedom to pursue and research concepts.

Higher education plays an indispensable role in society in research, development, and education. Most academic research will focus on collaborations and working as a team, both interdisciplinary and multilateral. Independence, individuality, and freedom of choice have unique characteristics in the higher education environment, with some limitations regarding collaborations and knowledge distribution. These attributes differ from the industry that widely contains trade secrets and is often vital to business growth, whereas higher education gives greater importance to research and development. Most research is conducted for learning purposes and yields little profit. Their goals tend to benefit in the longer term, leading to the differentiation in advancement between industries and educational institutions. Critical aspects of higher education are that researcher careers are usually individual, and the opportunities to be recognized for their accomplishments are more valuable than in the industry.

Instructional scaffolding has three steps which are 1) Model selection, 2) Breakdown, and 3) Encouragement or providing feedback. The model selection step is building interest to motivate students to be voluntarily interested in learning. This can be done by demonstrations, performances or showing how something is done, presentations, providing examples, using case studies, visualizing the desired goals, using words to motivate students, using questions to urge a warning, using the technology of motion pictures and sound for students to observe and analyze, etc. Educators are the ones to choose the appropriate techniques for the learning level of students. The breakdown step is the most difficult. It breaks down activities into subtasks to clarify work in simplified steps. Reducing the size of the work down from easy to hard work as if the educator is generating the dots or constantly giving support, and the students are the dot connectors through mutual aid with a goal that students can perform their work which they are not able to carry out on their own. However, this assistance will gradually change and decrease while the students gradually increase their abilities to perform independently. Before activity breakdown, the educator should find the missing gap to revise which activities students still can and cannot perform so the educator can focus exclusively on the activities that cannot be achieved, which may use skill-building methods, knowledge, vocabulary choice, appropriate language, tips and tricks, special techniques, strategies, presenting obstacles or problems that could occur, inspiration, etc. The encouragement or feedback, or cheer-up step, could be done with compliments, giving opinions, analyzing strengths and weaknesses, constructive criticism, providing advice for improvement, etc.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

**Table 1.**
Synthesizing a virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

| Topic | Activities | Reviews |
|---|---|---|
| Virtual Team Collaboration | Collaborative | Bai, et al. [1]; Herrera-Pavo [2]; Kankaew and Wannapiroon [3]; Kolm, et al. [6]; Yoon and Chang [11] and Zaphiris and Andri [12] |
| | Networking | |
| | Responsibility | |
| | Knowledge | |
| | Skill | Alves, et al. [7] and Baidya, et al. [8] |
| Network Simulators | Platform | |
| | Tools | |
| | Throughput | |
| Cybersecurity Competency | Identify | Alammari, et al. [9]; Bock, et al. [10]; Katsantonis, et al. [13] and Sánchez-Torres, et al. [14] |
| | Detect | |
| | Protect | |
| | Respond | |
| | Recovery | |
| Cyber Security Threat | CyberSec Technology | Alves, et al. [7]; Baidya, et al. [8]; Katsantonis, et al. [13]; Liu, et al. [15] and Ulven and Wangen [16] |
| | Cyber Defense | Yoon and Chang [11] |
| Higher Education | Cyber Security Threats Competency | Ashmawy and Schreiter [17]; Bai, et al. [1]; Chen and Kuo [18]; Chen and Zhu [19]; Du and Zeng [20]; Kolm, et al. [6]; Sánchez-Torres, et al. [14] and Ulven and Wangen [16] |
| | Knowledge | |
| | Skill | |
| | Attitude | |

Table 1, synthesis results of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students, comprises five main factors and 19 subfactors. Aspect 1 Virtual Team Collaboration comprises five subfactors, i.e., Collaborative, Networking, Responsibility, Knowledge, and Skill. Aspect 2 Network Simulators comprise three subfactors, i.e., Platforms, Tools, and Throughput. Aspect 3 Cybersecurity competency comprises five subfactors, i.e., Identify, Protect, Detect, Respond, and Recovery. Aspect 4 Cyber Security Threat comprises two subfactors, i.e., CyberSec Technology and Cyber Defense. Aspect 5 Higher Education comprises four subfactors, i.e., Cyber Security Threats, Competency, Knowledge, Skill, and Attitude.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

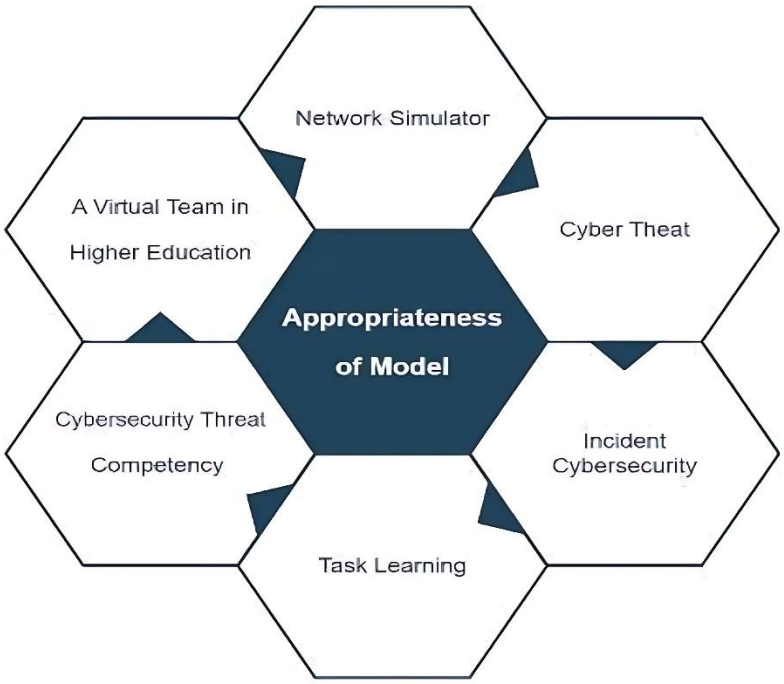


**Figure 1.**
The conceptual framework of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

The conceptual framework of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students began from virtual team collaborations of higher education students dividing work duties according to the process and purpose to propose for a method [13] to choose network simulators. Studying cybersecurity from previous cyber threat incidents and then learning to follow the action plan counts for greater cybersecurity competency from cyber threats. They are studying relevant research and designing the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students. Afterward, the designed model is evaluated by the experts.

Research Instruments the virtual team collaboration model uses network simulators to develop cybersecurity competency for higher education students. Feasibility evaluation of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

Data Collection First The process involves preparing invitation letters and feedback forms for experts to assess their expertise. The experts' evaluation and an assessment of the feasibility of a virtual team collaboration model using network simulators will be used to enhance the cybersecurity competency of higher education students. Step The data collected from the feasibility evaluation of the virtual team collaboration model using network simulators to improve the cybersecurity competency of higher education students will be divided into three areas, collected from the seven experts involved. Step 3 The results of the feasibility evaluation of the virtual team collaboration model using network simulators to enhance the cybersecurity competency of higher education students will be summarized and improved upon.

## 3. Results Results

Study results of the conceptual framework of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

Development results of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students that occurred from the evaluation of model feasibility by two experts on virtual collaboration, two experts on network simulators, and three experts on cybersecurity competency for higher education students. There are seven experts with a minimum of a 5-year of experience in their expertise at an excellent level.

Design results of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students.

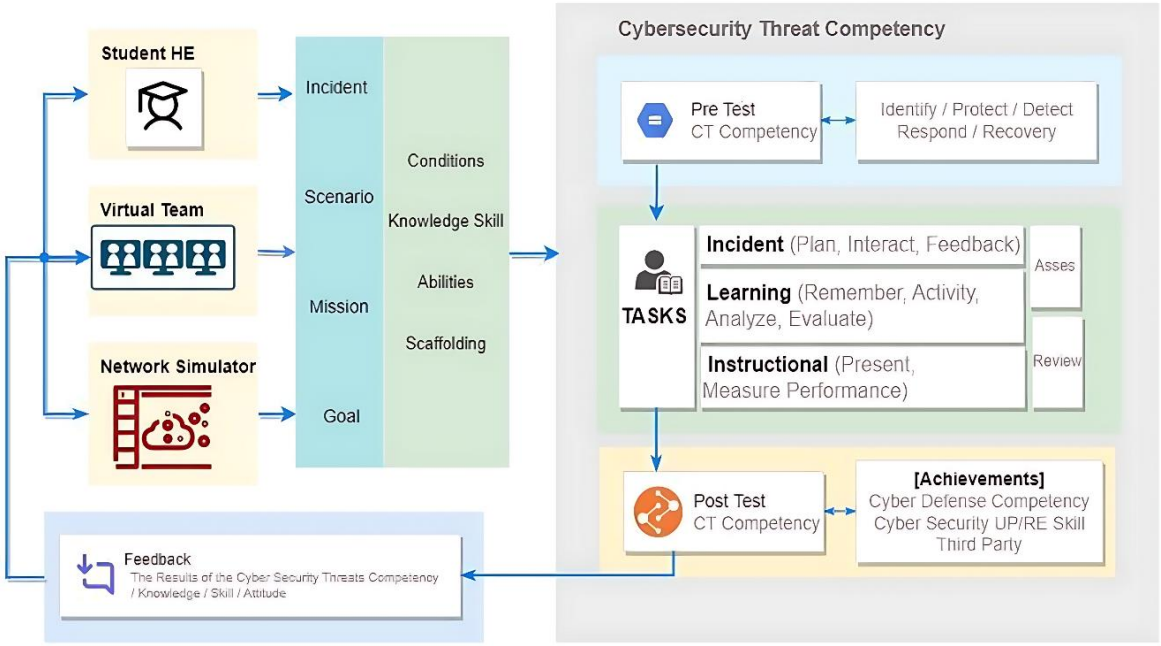


**Figure 2.**
A virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students (VTCyberThreat).

### *3.1. Model Approach*

The virtual team collaboration model uses network simulators to develop cybersecurity competency for higher education students. The process of the system, as shown in Figure 2, is separated into six steps as below.

Preparation: Student HE is a group of higher education students. Virtual Team is building a team for learning and dividing educational duties as planned. Network Simulator is a program for educational use either offline or online.

Studying the incidents of cyber threats, narratives, missions, and purposes within the team to identify conditions, skills, knowledge, and learning styles within the group.

Perform a pre-test assessment of identifying, detecting, protecting, responding, and recovering to collect students' results.

Studying how to prevent cyber threats from previous cyber threat incidents learning how to act according to the teamwork plan to improve cybersecurity competency from threat incidents. Competency results are knowledge, skills, and the ability to prevent cyber threats and manage them efficiently while measuring team performance.

Perform a post-test assessment to evaluate performance from competency, knowledge, skills, and abilities to prevent cyber threats and manage them efficiently.

Applying the results to improve better cyber threat incidents, narratives, missions, and purposes.

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

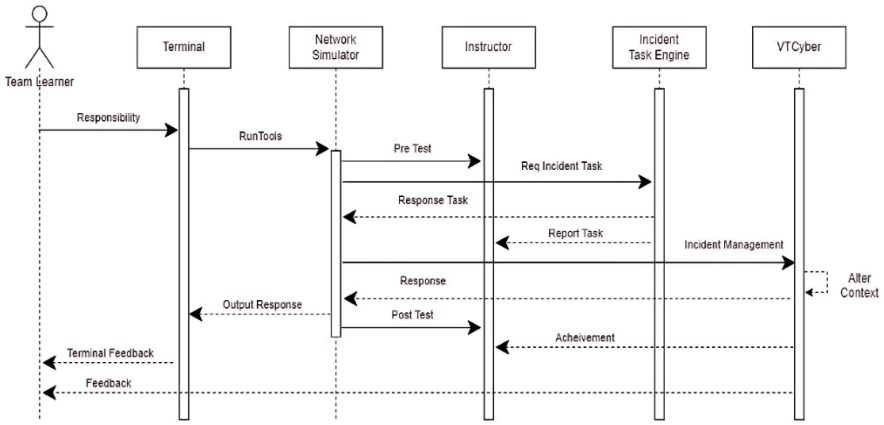


**Figure 3.**
Sequence Diagram of the Model Approach.

This model approach indicates the main components that should be considered in designing a cybersecurity system accompanied by an interconnection of these components in the structure of cyber threat incidents. The model's key concept is actions geared towards fulfilling incidents that exceed targeted attacks. Students should comply with the previously indicated implementable sequence for successful management according to the current limitations and conditions. Student progress will be examined, and their efforts will be supported through teaching materials and guidance preparations. Lastly, student efficiency is evaluated, reviewed, and provided with feedback. The objectives of learning the educational environment and learning strategies are to facilitate elemental analysis in studying cybersecurity by the activity theory model.

**Table 2.**
Process of the Model Approach.

| Process | Description | Technology | Evaluation |
|---|---|---|---|
| Cyber Security Threat Competency | Incident | Virtual Team Collaboration Network Simulator | Identify, Detect, Protect, Respond, Recover |
| | Scenario | | |
| | Mission | | |
| | Goal | | |
| | Conditions | | |
| | Knowledge Skill | | |
| | Abilities | | |
| | Scaffolding | | |
| Cyber Security Threat Learning | Study Task | Virtual Team Collaboration Network Simulator | Capture the Flag, Open Source, Incident Logs Responsibilities |
| | Division of responsibilities | | |
| | Incident Case | | |
| | Plan | | |
| | Interact | | |
| | Feedback | | |
| | Activity | | |
| | Analyze | | |
| | Evaluate | | |
| | Measure Performance | | |
| | Review | | |
| Competency in Cybersecurity | Achievements | New Cyber Security Technology | Cyber Defense Competency, Cyber Security Up/Re Skill, Third Party, ChatGPT |
| | Cyber Defense Competency | | |
| | Cyber Security UP/RE Skill | | |
| | Third Party | | |
| Data Feedback | Achievements | Virtual Team Collaboration | The Results of the Cyber Security Threat Competency, Knowledge, Skill, Attitude |

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 6: 2203-2212, 2025*
*DOI: 10.55214/25768484.v9i6.8336*

The feasibility evaluation of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students by experts is shown in Table 2.

## 4. Discussion and Conclusion

The feasibility evaluation of the virtual team collaboration model using network simulators to develop cybersecurity competency for higher education students by experts is shown in Table 3.

**Table 3.**
The Appropriateness of the VTCyberThreat Model with Cyber Security Threat Learning.

| Part of Description | Result | | Rate of Appropriateness |
|---|---|---|---|
| | Mean | S.D. | |
| Input Preparation | 4.78 | 0.44 | Excellent |
| Studying the sequence of cyber security threat incidents | 4.78 | 0.44 | Excellent |
| Studying the prevention of cyber threats from previous cyber threat incidents | 4.89 | 0.33 | Excellent |
| Cybersecurity competency from threat incidents | 4.89 | 0.33 | Excellent |
| Success from competency, knowledge, skills, and abilities to prevent cyber threats and manage them efficiently. | 4.89 | 0.33 | Excellent |
| The model can be used with coursework of higher education students to improve competency in preventing cyber threats. | 4.89 | 0.33 | Excellent |
| Total | 4.85 | 0.33 | Excellent |

The working model of VTCyberThreat is a visual approach to developing a learning and training approach regarding efficient cybersecurity. Cybersecurity education would aid in training skills for the predetermined response plan for cyber threat incidents. Moreover, this model presentation contains examples excerpted from many steps of situation prototypes to reveal practical design details. Researchers evaluated the approach from two experts on virtual team collaboration, two experts on network simulators, and three experts on cybersecurity competency for higher education students. Therefore, seven experts studied the approach per the component extraction model. The preliminary assessment should be supported as the VTCyberThreat model has assembled the essential characteristics indicated in the learning approach, like a cybersecurity game. The presented evaluation shows that the VTCyberThreat model can provide actual student experiences, while the well-arranged educational environment has definite learning objectives and a proper assessment. Furthermore, this model can also be utilized on the cloud system as the network simulator program can be accessed online.

## Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

## Copyright:



## References

[1] W. Bai, Z. Pan, S. Guo, Z. Chen, and S. Xia, "MDC-Checker: A novel network risk assessment framework for multiple domain configurations," *Computers & Security*, vol. 86, pp. 388-401, 2019. https://doi.org/10.1016/j.cose.2019.06.016

[2] M. Á. Herrera-Pavo, "Collaborative learning for virtual higher education," *Learning, Culture and Social Interaction*, vol. 28, p. 100437, 2021. https://doi.org/10.1016/j.lcsi.2020.100437

[3] V. Kankaew and P. Wannapiroon, "System architecture for virtual team campus on cloud to support internal quality assurance of Rajamangala university of technology," *International Journal of Online and Biomedical Engineering*, vol. 15, no. 7, pp. 99-110, 2019. https://doi.org/10.3991/ijoe.v15i07.10414

[4] Risk Based Security, "2020 data breach quickView report. Risk Based Security," 2020.
[5] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape report 2019. ENISA, European Union," 2019.
[6] A. Kolm *et al.*, "International online collaboration competencies in higher education students: A systematic review," *Journal of Studies in International Education*, vol. 26, no. 2, pp. 183-201, 2022.
[7] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of SCADA testbeds for cybersecurity research: A modular approach," *Computers & Security*, vol. 77, pp. 531-546, 2018. https://doi.org/10.1016/j.cose.2018.05.002
[8] S. Baidya, Z. Shaikh, and M. Levorato, "FlyNetSim: An open source synchronized UAV network simulator based on ns-3 and ardupilot," in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2018, pp. 37-45.
[9] A. Alammari, O. Sohaib, and S. Younes, "Developing and evaluating cybersecurity competencies for students in computing programs," *PeerJ Computer Science*, vol. 8, p. e827, 2022. https://doi.org/10.7717/peerj-cs.827
[10] K. Bock, G. Hughey, and D. Levin, "King of the Hill: A novel cybersecurity competition for teaching penetration testing," in *Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON). IEEE*, 2019.
[11] K. Yoon and S.-Y. Chang, "Teaching team collaboration in cybersecurity: A case study from the transactive memory systems perspective," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021: IEEE, pp. 841-845.
[12] P. Zaphiris and I. Andri, *Learning and collaboration technologies*. Cham: Springer International Publishing, 2016.
[13] M. N. Katsantonis, I. Mavridis, and D. Gritzalis, "Design and evaluation of cofelet-based approaches for cyber security learning and training," *Computers & Security*, vol. 105, p. 102263, 2021. https://doi.org/10.1016/j.cose.2021.102263
[14] B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart campus: Trends in cybersecurity and future development," *Revista Facultad de Ingeniería*, vol. 27, no. 47, pp. 93–101, 2018. https://doi.org/10.19053/01211129.v27.n47.2018.7807
[15] C.-W. Liu, P. Huang, and H. Lucas, "IT centralization, security outsourcing, and cybersecurity breaches: Evidence from the US higher education," 2017.
[16] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, pp. 1–40, 2021.
[17] A. K. Ashmawy and S. I. Schreiter, "EEE education society, & institute of electrical and electronics engineers," in *Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON): Date and Venue, 9–11 April, 2019, Dubai, UAE. IEEE*, 2019.
[18] C.-M. Chen and C.-H. Kuo, "An optimized group formation scheme to promote collaborative problem-based learning," *Computers & Education*, vol. 133, pp. 94-115, 2019. https://doi.org/10.1016/j.compedu.2019.01.011
[19] L. Chen and W. Zhu, "Autonomous mobile learning model of cloud education based on intelligent algorithm of wireless network communication," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 1144767, 2021. https://doi.org/10.1155/2021/1144767
[20] W. Du and H. Zeng, "The SEED internet emulator and its applications in cybersecurity education," *arXiv preprint arXiv:2201.03135*, 2022.