Enhancing Workforce Cyber Resilience: Bridging the Gap in ICS Protection

Abdullah Jawad*, Noah Quesenberry†, Husnu S. Narman‡, and Paulus Wahjudi§
Email: *jawad1@marshall.edu,†quesenberr22@marshall.edu,‡narman@marshall.edu,§wahjudi@marshall.edu

***Abstract*—Protecting critical infrastructure is a key challenge in cyber resilience, particularly when it comes to safeguarding Industrial Control Systems (ICS). The workforce responsible for this protection comprises two distinct groups: ICS Engineers and IT/Cybersecurity Specialists. ICS Engineers design, implement, and maintain operational technology and networks but often lack expertise in cyber threat intelligence. Conversely, IT/Cybersecurity Specialists focus on securing systems against vulnerabilities and attacks but usually lack knowledge of operational technology concepts. This gap in expertise can leave critical infrastructure vulnerable to cyber threats. To address this issue, modern teaching approaches are being developed to enhance the workforce's cyber resilience. These approaches aim to provide comprehensive training that bridges the knowledge gap between ICS Engineers and IT/Cybersecurity Specialists. By integrating cyber threat intelligence into the training of ICS engineers and operational technology concepts into the training of IT/Cybersecurity Specialists, these educational strategies seek to create a more cohesive and capable workforce. This article reviews these contemporary teaching methods and evaluates their effectiveness in preparing the workforce to handle cybersecurity threats to critical infrastructure.**

***Index Terms*—Industrial Control Systems, Cybersecurity, Education**

I. Introduction

In the modern digital era, the security of critical infrastructure has emerged as a paramount concern for governments and industries worldwide. Industrial Control Systems (ICS), which manage and control essential services such as electricity, water, transportation, and manufacturing, are increasingly interconnected with corporate networks and the Internet [1]. This integration, while improving operational efficiency, has expanded the attack surface for cyber threats. High-profile incidents such as the Stuxnet worm and the Ukrainian power grid attack have underscored the potential for cyber adversaries to cause significant disruption and damage through ICS vulnerabilities. The responsibility of safeguarding these systems falls upon a workforce divided into two specialized domains: ICS Engineers and IT/Cybersecurity Specialists. ICS Engineers possess deep expertise in designing, implementing, and maintaining operational technologies and networks. Their focus is on ensuring the reliability, efficiency and safety of the system. However, they often lack comprehensive training in cyber threat intelligence and advanced cybersecurity practices. On the other hand, IT/Cybersecurity Specialists are adept at identifying and mitigating vulnerabilities within traditional IT environments but may not fully grasp the complexities and unique characteristics of operational technologies used in ICS. This dichotomy in expertise creates a critical gap in the overall defense strategy against cyber threats targeting critical infrastructure.

The convergence of IT and operational technology (OT) environments requires a workforce that is proficient in both domains. The lack of cross-disciplinary knowledge not only hinders effective communication and collaboration between ICS Engineers and IT/Cybersecurity Specialists but also leaves critical infrastructure susceptible to sophisticated cyberattacks. Adversaries can exploit this gap, using advanced tactics to bypass conventional security measures and infiltrate ICS environments [2].

To address this pressing issue, innovative educational approaches are being developed to enhance the cyber resilience of the workforce responsible for protecting critical infrastructure. These modern teaching methods aim to bridge the knowledge gap by integrating cybersecurity principles into the training of ICS Engineers and introducing operational technology concepts to IT/Cybersecurity Specialists. By fostering a comprehensive understanding of both disciplines, these educational strategies seek to cultivate a workforce capable of collaboratively defending against evolving cyber threats.

This paper explores contemporary teaching methodologies designed to improve cyber resilience of the workforce in the context of ICS protection. We review some recent critical infrastructure attacks in the United States and evaluate the some of the vulnerabilities in the training of the cyber workforce. Then, we review various educational programs, training initiatives, and curricular innovations that aim to equip professionals with the necessary skills and knowledge to secure critical infrastructure effectively. Then we look at some recent research literature with the specific agenda to improve training activities for cybersecurity in ICS and critical infrastructure. Furthermore, we evaluate the effectiveness of these approaches in preparing the workforce to anticipate, withstand, and recover from cybersecurity threats. By identifying best practices and areas for improvement, this study contributes to ongoing efforts to fortify the defenses of critical infrastructure against the ever-increasing landscape of cyber risks. Lastly, we will evaluate a recent research activity conducted at Marshall University where a group of students were trained on a CyberHive (Industrial Control Systems Simulation) for ICS security and the students were then divided into groups and were to participate in a capture the flag activity and the scores of the groups of students statistically reviewed to evaluate whether Cybersecurity and Critical Infrastructure Cybersecu-

rity Challenges have any correlation with one another.

The remainder of this paper is organized as follows: Section II discusses the recent ICS related attacks. Section III highlights various learning tools and concept for cybersecurity. Section IV discuss the case study to observe the effects of CyberHive ICS on the performance of students. Finally, Section V has the final remarks.

II. ICS Attacks and Vulnerabilities in the Systems

Recent incidents in the United States have highlighted significant vulnerabilities within ICS environments, underscoring the urgent need for enhanced security measures and workforce preparedness. One of the most prominent attacks occurred in May 2021, when the Colonial Pipeline, one of the largest fuel pipelines in the United States, fell victim to a ransomware attack orchestrated by the cybercriminal group DarkSide. The attackers infiltrated the company's IT network and deployed ransomware, encrypting critical data, and forcing the pipeline's operators to proactively shut down operations to prevent the malware from spreading to the OT network. This incident led to massive fuel shortages and raised gasoline prices across the East Coast, demonstrating the profound impact that ICS cyber-attacks have on national security and the economy. The Colonial Pipeline attack exposed vulnerabilities related to network segmentation and the lack of robust incident response plans that bridge IT and OT environments [3].

In the early part of February 2021, a cyber-attack targeted a water treatment facility in Oldsmar, Florida. An unknown attacker remotely accessed the facility's control systems via poorly secured remote access software and attempted to increase the levels of sodium hydroxide (lye) in the water supply to dangerous levels. Fortunately, a plant operator noticed the unauthorized changes and quickly reversed them, preventing any harm to the public. This incident highlighted vulnerabilities in remote access protocols, insufficient authentication mechanisms, and the lack of real-time monitoring and alerts within ICS environments [4].

In 2022 and 2023, there has been a continued rise in ransomware and supply chain attacks targeting critical infrastructure. For instance, the Cybersecurity and Infrastructure Security Agency (CISA) issued alerts regarding increased cyber threats from state-sponsored actors targeting ICS and supervisory control and data acquisition (SCADA) systems. These actors have developed tools specifically designed to scan, compromise, and control ICS devices, exploiting vulnerabilities such as outdated software, default configurations, and inadequate network segmentation [5].

The increased connectivity between IT and OT systems has blurred the traditional boundaries, making ICS environments more accessible to cyber threats originating from the internet. Vulnerabilities often stem from legacy systems that were not designed with cybersecurity in mind, reliance on proprietary protocols lacking encryption, and insufficient authentication and authorization mechanisms. Additionally, the adoption of Industrial Internet of Things (IIoT) devices introduces new entry points for attackers, as these devices may have limited security features and are often overlooked in security assessments [2].

These vulnerabilities are exacerbated by a workforce that may not be fully equipped to address the unique challenges of securing ICS environments. ICS Engineers may lack cybersecurity expertise, while IT/Cybersecurity Specialists might not fully understand the operational requirements and constraints of ICS. This skills gap contributes to inadequate security practices, such as improper configuration of devices, delayed patch management, and failure to implement defense-in-depth strategies. The recent attacks and identified vulnerabilities underscore the critical need for a holistic approach to ICS security. This involves not only technological solutions but also enhancing the skills and knowledge of the workforce responsible for protecting these systems. By fostering cross-disciplinary expertise and promoting collaboration between ICS Engineers and IT/Cybersecurity Specialists, organizations can better safeguard critical infrastructure against evolving cyber threats.

III. Literature Review – Closing the IT/OT Gap

A. Enhancing Academic Teaching Methods

Cyber resilience is increasingly critical for securing essential infrastructures like energy and communication networks, which are prime targets for sophisticated cyberattacks. A study [6] conducted at the Nagoya Institute of Technology emphasized the ability of the organization to maintain operations during and after cyber incidents, especially in sectors heavily dependent on ICS. Using the Red Team-Blue Team framework, a well-established cybersecurity training exercise that simulates real-world attack and defense scenarios, the study provides critical insights into incident management, decision-making processes, and organizational resilience. The Blue Team, tasked with defending a simulated chemical plant, had to detect and respond to attacks while managing operational tasks. A key finding was the dynamic shift in defense activities as the incident progressed: initially focusing on preventive measures, the Blue Team had to rapidly reallocate resources toward detection and response as the attack escalated. The study highlights that a top-down decision-making structure limited the team's flexibility, hindering effective response to the rapidly changing attack environment and leading to delays and inefficiencies.

Lack of communication between management and lower-level team members further slowed response time, underscoring the importance of adaptive management and decentralized decision-making during crises. To address these challenges, the study suggests [6] integrating resilience engineering frameworks into cybersecurity training and incident management to better assess and improve organizational performance. It recommends moving away from rigid management structures toward collaborative decision-making with open communication across all team levels to enable faster, more coordinated responses. Improved resource management is also crucial for adapting to escalating situations; by viewing cyber incident

responses as dynamic resource allocation problems, organizations can develop more effective strategies for managing multiple, parallel tasks under crisis conditions. For future research, the authors propose developing detailed performance evaluation frameworks that track both technical effectiveness and human resource management during incidents. They also suggest that future exercises focus on complex, multifaceted scenarios to test organizational resilience under realistic conditions, helping organizations better prepare for real-world attacks as cyber threats become more sophisticated, particularly in critical infrastructure sectors where disruptions can have widespread consequences.

Gamification of critical infrastructure cybersecurity scenarios was also considered a potential solution to help improve the workforce. Research conducted at Purdue University [7] introduced the Network Defense Training Game (NDTG), an innovative gamified training platform aimed at addressing the shortage of skilled cybersecurity professionals in critical infrastructure sectors. By highlighting the increased vulnerabilities due to the convergence of OT and IT networks—where once-isolated systems like ICS were now exposed to cyber threats—the research underscored the urgent need for effective training solutions. NDTG applied gamification techniques, incorporating elements such as simulation, competition, and problem-solving to enhance engagement and facilitate practical learning. Players were immersed in realistic cybersecurity scenarios modeled after real-world incidents, where they had to strategically allocate resources and implement security controls under budget constraints to defend against simulated attack vectors like rogue devices, misconfigurations, third-party attacks, and insider threats. The game was structured around the NIST Cybersecurity Framework (CSF) and aligned with the National Institute of Standards and Technology's NICE Framework, ensuring that learning objectives were mapped to specific workforce roles. By combining best practices from cybersecurity frameworks with the engaging, practical learning environment provided by gamification, thereby equipping professionals with the necessary skills to defend critical infrastructure against sophisticated cyberattacks.

The use of Modern technology such as AI, Machine learning and extended reality can used to generate real world environments to train the students and professionals on academic topics this idea was explored in the study titled "Navigating Cybersecurity Training: A Comprehensive Review" explored various methods used in cybersecurity awareness training, analyzing both traditional techniques—such as passive awareness campaigns and classroom-based learning—and innovative approaches like simulation-based and app-based methods [8]–[10]. It highlighted the significant cybersecurity risks that had intensified with increased reliance on digital platforms, especially post-COVID-19, and noted that traditional methods often suffered from low engagement and poor knowledge retention [11]. To address these challenges, the study examined emerging trends involving Artificial Intelligence (AI), Machine Learning (ML), and Extended Reality (XR), which offered potential for automating risk identification, personalizing training content, and creating immersive learning environments, albeit with concerns over cost and scalability. A comparative analysis based on metrics like cost, scalability, engagement, and retention suggested that a blended approach combining the strengths of multiple methods could provide more effective training solutions. Implementation challenges such as resource allocation, continuous content updates, employee engagement, and the lack of effective metrics were discussed, with recommendations to incorporate real-world simulations, gamification, and interactive content to improve participation and knowledge retention. The study concluded by emphasizing the necessity for flexible and adaptive training strategies that leverage technological advancements to keep pace with evolving cyber threats, offering valuable insights into the current landscape and future directions of cybersecurity training [12].

While there are several available suggested approaches to enhance the training of the cyber security workforce there is need for an evaluation model to check the awareness of the workforce. The study titled "Towards an Innovative Model for Cybersecurity Awareness Training" introduced the Integrated Cybersecurity Awareness Training (iCAT) model, which leveraged multiple methods—such as knowledge graphs, serious games, gamification, and micro-learning modules—to create a comprehensive and flexible cybersecurity awareness training system. The iCAT model addressed the challenges organizations faced in keeping up with rapidly evolving cybersecurity threats by enhancing user engagement, improving knowledge retention, and providing adaptability in training efforts. It combined elements from previous successful training methods into a unified framework that included serious games to immerse participants in real-world scenarios, knowledge graphs to organize complex concepts, gamified learning management systems with leaderboards and real-time feedback, Capture the Flag components for competitive challenges, and micro-learning modules that broke down complex topics into digestible lessons. The model offered significant advantages over traditional training by personalizing the learning experience based on participants' skill levels, providing immediate feedback, and allowing learners to progress at their own pace. Evaluations of the iCAT model demonstrated its effectiveness in improving participant engagement and knowledge retention. The study suggested future research directions, including empirical validation in different organizational settings, exploring scalability across industries, and integrating advanced technologies like artificial intelligence and augmented reality into the framework. This innovative approach presented a promising solution to improve the effectiveness and accessibility of cybersecurity awareness training programs [13].

B. Enhancing Professional Training Methods/Systems

Training professionals is different from a classroom environment as the possibility of error can have real consequences hence the training of professionals is more application based compared to the classroom. The study [14] provided an extensive review of cybersecurity training methods and solutions targeted toward Critical Infrastructure Protection (CIP), focus-

ing on the energy, aviation, and nuclear sectors. It evaluated existing training solutions in terms of methodologies, target groups, focus areas, and Key Performance Indicators (KPIs) used for measuring effectiveness, highlighting challenges such as increasing vulnerabilities due to digitalization, human error from lack of formal training, and the absence of standardized training methods. The study emphasized that traditional classroom-based training often lacked real-world application, advocating for hands-on, simulation-based training like red-teaming and cyber-warfare exercises, which were more effective for CIP personnel. Sector-specific approaches were analyzed, noting unique challenges in each: evolving training programs in aviation, the impact of smart grids introducing vulnerabilities in energy, and a shift from physical to cybersecurity focus on nuclear training. Essential KPIs identified for evaluating training effectiveness included user performance metrics, incident reduction metrics, and user feedback, while acknowledging challenges like resource limitations and diverse target audiences requiring customized solutions. The authors concluded that simulation-based and hands-on training provided the most effective learning experiences for CIP personnel and recommended future research to integrate different training methodologies, standardize evaluation criteria, and develop more sector-specific solutions to address the unique challenges faced by different critical infrastructure sectors [14].

As stated previously, ICS face an array of cybersecurity challenges, many of which stem from the increasing convergence of IT and OT. These Challenges are further compounded by the growing complexity of ICS and a notable disconnect between IT and OT groups. In [15], Khan et al. propose a practical cyber range to tackle and diminish the disconnect between IT and OT. Their proposed solution centers on a "real-time attacker defender gameplay model" in conjunction with dynamic and realistic simulations of typical ICS models. To enhance cyber awareness for OT operators, the authors' solution focuses on increasing their familiarity with attacker Tactics, Techniques, and Procedures (TTPs) to better detect and respond to cyber-attacks. For IT operators, the training for IT operators focuses on the use and awareness of ICS equipment, protocols, and overall system operation to help the operators better understand the potential impacts of cyber-attacks on ICS. Once both teams have gained more familiarity with the topics discussed, the operators are placed in the simulated environment. In this, a virtualized IT/OT network is utilized which is meant to model a typical corporate environment including components like external firewall, DMZ, SOC, SCADA, and OT networks. The simulation models a red vs blue team simulation in which IT and OT operators work together to stop the attack and successfully defend the network. The proposed solution, CR-ICS, includes details on attacker methodology and what steps to include in the training to ensure both IT/OT operators must apply what they previously learned in order to successfully defend the network. Through this simulation, OT operators gain hands on experience with offensive and defensive security tools as well as IT protocols and systems; therefore, the OT operators gain a deeper understanding of the IT perspective. On the other hand, IT operators will gain exposure to OT protocols, equipment, and processes necessary to carry out OT operations. Through this, IT operators will also be able to establish a normal baseline for operations and system behavior, but more importantly they will better understand the real-world consequences of cyberattacks on industrial systems. By training together and collaborating in this training, IT and OT operators can bridge knowledge gaps, enhance communication, and develop effective strategies for defending critical infrastructure against increasingly sophisticated cyberattacks [15].

The introduction of artificial intelligence has brought new approaches to OT and IT cyber-attack detection that were previously unavailable. One study [16] investigated the application of Ensemble Learning (EL) methods to enhance anomaly detection in Cyber-Physical Systems (CPS), which face increased vulnerabilities due to the integration of OT and IT networks in Industry 4.0. Traditional anomaly detection approaches, often designed for IT networks, were inadequate for CPS because of their complexity and the scarcity of real-world data. The authors proposed a hybrid anomaly detection model that combined signature-based detection for known threats, threshold-based detection for immutable CPS characteristics, and behavior-based detection using EL techniques such as voting, stacking, bagging, and boosting. By leveraging multiple classifiers—including Logistic Regression, Naïve Bayes, Support Vector Machines, K-Nearest Neighbor, and Multi-Layer Perceptron—the EL approach improved predictive performance, addressing challenges like high heterogeneity and class imbalances in CPS data. Experimental results using the Edge-IIoTset2023 and CICIoT2023 datasets demonstrated that EL methods provided a 4–7% improvement in predictive accuracy over traditional machine learning models, with boosting techniques particularly effective in minimizing false positives and negatives. The study underscored the critical importance of enhancing anomaly detection in CPS due to the severe consequences of interruptions in critical infrastructure and suggested future research directions, including the development of deep learning models, decision threshold tuning, and hybrid models combining OT and IT detection methods. This study contributed to a valuable methodology for improving CPS security by addressing unique challenges through a robust, ensemble-based approach. This study shows how AI and Machine learning can be used to better protect our systems and change the legacy approaches in the Critical Infrastructure cyber security [16].

Certain infrastructures such communication technologies link the OT and IT devices together, and certain attacks target the communication system to destroy the operational capability of the critical infrastructure. The study [17] presented a novel framework designed to address the cybersecurity challenges posed by the evolution of 5G technology. Recognizing that 5G networks introduced complex vulnerabilities and cyber threats due to their distributed architecture and integration of new technologies like Massive MIMO and IoT devices, the

authors developed Cyber5Gym to fill the gap in specialized cybersecurity training. This integrated, open-source, cloud-deployable cyber range enabled professionals to engage in hands-on cybersecurity training specifically tailored for 5G infrastructures. Key components of the framework included 5G network emulation using Open5GS and UERANSIM, attack simulation with 5Greplay to replicate various cyberattacks such as SMC replay attacks, DDoS, and DoS attacks, and the use of automation and virtualization through Docker and Shell scripts for scalable deployment. The framework offered significant advantages like scalability, reproducibility, and comprehensive training by simulating real-world attack scenarios in a realistic 5G environment. Evaluation of Cyber5Gym involved deploying it on Naver Cloud with 20 trainees managing simulated 5G networks, demonstrating its effectiveness in preparing cybersecurity professionals to handle 5G-specific threats. The study concluded by suggesting future research directions, including integrating more advanced attack scenarios, exploring AI and machine learning for threat detection and mitigation, and enhancing the training environment's realism and scalability through technologies like Kubernetes and hybrid virtualization models. This study contributed to a valuable tool for critical infrastructure cybersecurity training by addressing the growing complexity of modern telecommunications infrastructures and the emerging cyber threats they faced [17].

IV. Study Conducted at Marshall University using a SCADA System Simulation

At Marshall University a junior/senior level class titled "Cybersecurity" is taken by undergraduate students yearly in Spring semesters. Most of this class are computer science major students along with some cybersecurity major students in the class as well. For a lot of these students this is the first cybersecurity class with skill application as they can participate in the National Cyber League (NCL) as part of their class grade (extra curriculum activity). NCL is a cybersecurity competition designed to help students at various skill levels practice and demonstrate their abilities through hands-on exercises that simulate real-world cybersecurity scenarios. The NCL focuses on skill development in areas such as network traffic analysis, cryptography, password cracking, and web application security. It includes both individual and team competitions, beginning with the Preseason challenges, followed by Individual Games and Team Games, where participants collaborate to solve complex tasks. Participants are ranked on a national leaderboard based on their performance, providing recognition for their cybersecurity skills. The NCL is an educational platform that complements academic learning, offering practical experience for students in cybersecurity programs or those aspiring to enter the field. It caters to individuals with varying levels of expertise, from beginners to advanced players, helping them build relevant experience and enhancing their portfolios for internships and jobs in the cybersecurity industry [18].

Until Spring 2014, students gave the same criticism after participating that they were not prepared enough as the class teaches the theoretical aspects of cybersecurity but did not get into details about the practical implementation of these concepts in the NCL competition which has a lot of capture the flag (CTF) and application-based challenges with each category focusing on different aspects of cybersecurity.

A. Methodology

In Spring 2024, Marshall university invested in a CyberHive (SCADA system simulation), which is used for training industry professionals in maintaining critical infrastructure security [19]. The training is divided into several modules and after that as a test of their skills and knowledge the professionals would participate in a capture the flag simulation on the actual hardware components. The training was divided into several modules focusing on the following aspects; Understanding ICS/SCADA systems, Operational Technology Traffic Analysis, Vulnerability Analysis tools in Operational Technology and Exploitation of OT Networks (as shown in Table I).

TABLE I
The number of questions in each category.

Category	Number of Challenges
1 - ICS Basics	13
2 - PLC Programming	9
3 - Modbus Basics	6
4 - Modbus Analysis	5
5 - ENIP/CIP Basics	6
6 - Attack Surface Identification	10
7 - Static Analysis	5
8 - Dynamic Analysis	6
9 - Endpoint Manipulation	2

B. Team Perfomance from CyberHive CTF

These lab exercises were given to students as a part of the curriculum of their class, and they had to finish them before the deadlines. All these students had no experience with ICS / SCADA systems or Critical Infrastructure cybersecurity just like the NCL challenges that can be from any aspect of cybersecurity. After completing the training, the students were all divided into random groups tasked to participate in a mock CTF challenge [20]. The results of each group can be seen in Table II for the mock CTF.

TABLE II
Data of the teams from the CyberHive CTF challenge.

User Teams	Score	Completion Percentage
Team 1	2525	100%
Team 2	2525	100%
Team 3	1755	69.50&
Team 4	1715	67.92%
Team 5	1677	66.42%

After the CyberHive CFT challenge, the students were allowed to make their own teams just like all previous years and took the NCL which is a two-part challenge. While the ICS related modules from the CyberHive CTF were not closely

related to the topics of the NCL, the remaining topics such as Traffic Analysis, Vulnerability Analysis and Exploitation were closely linked to topics in the NCL (Scanning, Network Traffic analysis, and Enumeration and Exploitation). For the individual challenge game and then the team challenge game, the class was allowed to form their teams like previous years. After the NCL results were obtained, their performances were then compared to their peer performances from previous years.

Another observation made is majority of the challenges were solved by all the teams. There were a few that were difficult to solve for most teams as seen in Table III, which of are about 10 challenges were not completed by all teams. The Categories where most students faced the issue were Attack Surface Identification and Endpoint Manipulation.

TABLE III
THE PERCENTAGE OF SUBMITTED ANSWERS FOR EACH CATEGORY.

Category	Submission Rate
1 - ICS Basics	100%
2 - PLC Programming	95.5%
3 - Modbus Basics	100%
4 - Modbus Analysis	96%
5 - ENIP/CIP Basics	96.7%
6 - Attack Surface Identification	72%
7 - Static Analysis	100%
8 - Dynamic Analysis	100%
9 - Endpoint Manipulation	70%

C. Comparison of Students' Performance for Last Three Semesters (Springs 2022, 2023, and 2024)

The results of the NCL for Spring 2024, Spring 2023, and Spring 2022 can be seen in Figure 1, Figure 2, and Figure 3, respectively. In Spring 2024, there were a lot more teams compared to previous years. We believe that this was because after doing a mock CTF, the students were more confident in their abilities to do the NCL challenges [21]. Every year there are certain teams that do not attempt the NCL Team challenge as they do not have any completion percentage. In Spring 2024, about 26.6% of the teams did not attempt the challenge. This is more than previous years as the non-competing percentage for 2023 was 25% and for 2022 it was 16.6%. This data will not be included in the remaining analysis as it would reduce the actual average values of the results obtained [22].

The first thing that can be identified in Spring 2024, is that the average completion percentage of students was 43%. This is less than Spring 2023, the average completion percentage was 73%, and Spring 2022, the average completion percentage was 54%. Although the completion rate is important, it is possible that different cohorts have different schedules, which may prevent students from reserving time to complete the challenges. Therefore, we investigate the accuracy rate according to the completion rate for each year.

In Spring 2024, the average accuracy rate was 74%. This was significantly higher than previous years, where it was 66% in Spring 2023, and it was 40% in Spring 2022. This shows that in Spring 2024, the students were not trying trail-error

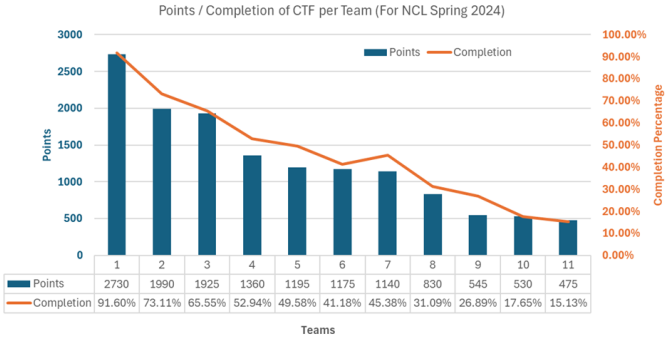

Fig. 1. Performance of students in terms of score and completion in Spring 2024 for NCL.

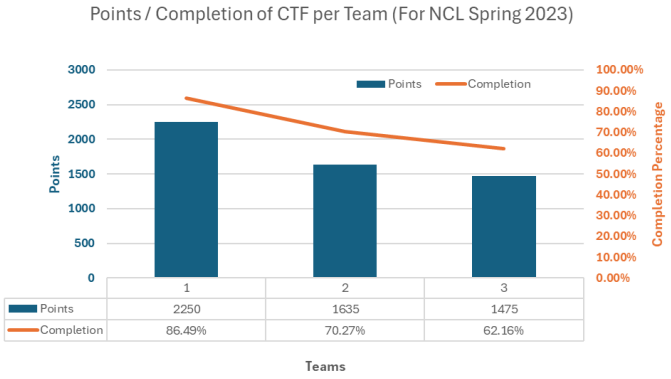

Fig. 2. Performance of students in terms of score and completion in Spring 2023 for NCL.

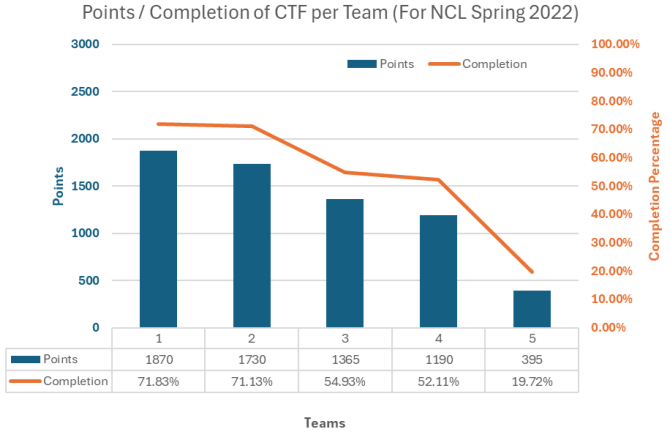

Fig. 3. Performance of students in terms of score and completion in Spring 2022 for NCL.

but were working on solutions to obtain the actual answer. The accuracy improvement shows that CyberHive CTF helped them prepare for the NCL challenge and provide experience to think about cybersecurity concepts that they did not have any knowledge before. Hence, they worked towards finding a correct solution.

V. Conclusion

Safeguarding critical infrastructure, especially Industrial Control Systems (ICS), is a significant challenge in cyber resilience. The workforce tasked with this protection includes ICS Engineers and IT/Cybersecurity Specialists, each with distinct expertise. ICS Engineers excel in designing and maintaining operational technology but often lack cyber threat intelligence skills. Conversely, IT/Cybersecurity Specialists are adept at securing systems but may not fully understand operational technology. This expertise gap can leave critical infrastructure vulnerable to cyber threats. To mitigate this, modern teaching approaches are being developed to enhance cyber resilience by bridging the knowledge gap between these two groups. By incorporating cyber threat intelligence into ICS Engineers' training and operational technology concepts into IT/Cybersecurity Specialists' education, these strategies aim to create a more cohesive and capable workforce.

In this study, we reviewed several training concepts such as gamification and awareness. Moreover, future research aims to validate its effectiveness across various organizational contexts and explore integration with advanced technologies. These exercises, training, and educational models can better hold the attention of students while bridging the most crucial gap for individuals learning about IT/OT, hands-on experience. As explained with the CyberHive training results at Marshall University, students were able to complete gamified lessons to practice their skills. Not only did this improve their understanding of ICS related topics, but it directly correlated to cybersecurity as students improved their accuracy rates on for Nation Cyber League. This demonstrated that there is a viable way to implement training for ICS that will improve understanding of base cybersecurity topics, which is an incredible stride in the movement of bridging the gap between IT and OT practitioners.

References

[1] "Recent cyber attacks on us infrastructure underscore vulnerability of critical us systems, november 2023–april 2024," Jun. 2024. [Online]. Available: https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

[2] M. G. Michail, C. Kolias, C. Kambourakis, C. Rieger, and J. Benjamin, "Vulnerabilities and attacks against industrial control systems and critical infrastructures," *arXiv*, pp. 1–40, 2021.

[3] "Fbi statement on compromise of colonial pipeline networks," 2021. [Online]. Available: https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

[4] J. Cervini, A. Rubin, and L. Watkins, "Don't drink the cyber: Extrapolating the possibilities of oldsmar's water treatment cyberattack," in *17th International Conference on Information Warfare and Security*, 2022, pp. 19–25.

[5] "Nsa partners with doe, cisa, and fbi to release advisory on apt cyber tools targeting ics/scada devices," Apr. 2022. [Online]. Available: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2997885/

[6] T. Aoyama, H. Naruoka, I. Koshijima, W. Machii, and K. Seki, "Studying resilient cyber incident management from large-scale cyber security training," in *Proceedings of the 10th Asian Control Conference*. IEEE, 2015, p. 3.

[7] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, "Gamification of cybersecurity for workforce development in critical infrastructure," *IEEE Access, vol. 10*, pp. pp. 112 487–112 501, 2022.

[8] N. Loftus, C. Green, and H. S. Narman, "The cybersecurity packet control simulator: Cspcs," in *2022 IEEE Global Humanitarian Technology Conference (GHTC)*, 2022, pp. 226–233.

[9] N. Loftus and H. S. Narman, "Use of machine learning in interactive cybersecurity and network education," *Sensors*, vol. 23, no. 6, 2023.

[10] E. M. Dillon, C. Carpenter, J. Cook, T. D. Wills, and H. S. Narman, "A machine learning-based automatic feedback system to teach cybersecurity principles to k-12 and college students," in *2022 IEEE Global Humanitarian Technology Conference (GHTC)*, 2022, pp. 219–225.

[11] J. Maddy, E. M. Dillon, and H. S. Narman, "Adapting cybersecurity teacher training camp to virtual learning," in *IEEE Integrated STEM Education Conference (ISEC)*, 2023, pp. 301–308.

[12] S. A.-D. Qawasmeh, A. A. S. AlQahtani, and M. K. Khan, "Navigating cybersecurity training: A comprehensive review," 2024. [Online]. Available: https://arxiv.org/abs/2401.11326

[13] H. Taherdoost, "Towards an innovative model for cybersecurity awareness training," *MDPI (Information)*, p. 19, 2024.

[14] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, vol. 40, 2021.

[15] S. Khan, A. Volpatto, G. Klara, J. Esteban, T. Pescanoce, S. Caporusso, and M. Siegel, "Cyber range for industrial control systems (cr-ics) for simulating attack scenarios," Sloan School of Management, Massachusetts Institute of Technology, Tech. Rep., 2021.

[16] N. Jeffrey, Q. Tan, and J. R. Villar, "Using ensemble learning for anomaly detection in cyber–physical systems," *Electronics*, vol. 13, no. 7, 2024.

[17] M. A. Hamza, U. Ejaz, and H.-c. Kim, "Cyber5gym: An integrated framework for 5g cybersecurity training," *Electronics*, vol. 13, no. 5, 2024.

[18] P. Wang and H. D'Cruze, "The role of cyber competitions in cyber defense education: A case study of national cyber league (ncl) participation," *Issues in Information Systems*, pp. 128–138, 2022.

[19] G. Yadav and K. Paul, "Architecture and security of scada systems: A review," *International Journal of Critical Infrastructure Protection*, 2021.

[20] S. Noor, O. Tajik, and J. Golzar, "Simple random sampling," *Internation Journal of Education & Language Studies*, 2012.

[21] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, 2021.

[22] J. Mandel, *Statistical Analysis of Experimental Data*. Courier Corporation, 2012.