2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #51624

MTU Superior Cyber Range: An Architectural and Strategic Overview for Cybersecurity Training and Workforce Development

Prof. Victoria Behringer Walters, Michigan Technological University

Victoria B. Walters is a Ph.D. Candidate in Computational Science and Engineering and a Professor of Practice in the Department of Applied Computing at Michigan Technological University. Her research focuses on the intersection of cybersecurity, law, and ethical computing, including areas like Information Governance and the ethical application of Generative AI in Penetration Testing. She also serves as a Security & Compliance Manager at HCLSoftware. Her work on the MTU Superior Cyber Range detailed in this paper is a core component of her broader efforts to advance scalable cybersecurity training and workforce development.

Noah Hansen, Michigan Technological University
Carter Ravenstone, Michigan Technological University
Alexander Jay Briggs, Michigan Technological University
Ethan Irwin Ashley, Michigan Technological University
August Staples, Michigan Technological University
Anders Thor Lien, Michigan Technological University

MTU Superior Cyber Range: An Architectural and Strategic Overview for Cybersecurity Training and Workforce Development

Abstract

This paper examines the educational impact and design of the MTU Superior Cyber Range, a scalable and portable cybersecurity training platform developed to address the growing need for accessible, hands-on cybersecurity education. The platform's pedagogical framework emphasizes experiential learning through realistic cyber defense scenarios, enabling students to develop critical competencies in threat detection, incident response, and security architecture. Our multi-node virtualization cluster architecture was designed with two primary educational goals: (1) providing authentic, industry-relevant training experiences across diverse educational settings, and (2) removing infrastructure barriers that limit cybersecurity education access in under-resourced institutions.

We evaluated the platform's educational effectiveness through a proof-of-concept deployment at a local high school in Spring 2025. Using pre and post skill assessments, student surveys, and instructor feedback, we measured improvements in cybersecurity knowledge, student engagement, and self-efficacy in technical problem-solving. Preliminary results indicate significant gains in students' ability to identify vulnerabilities and apply defensive strategies, along with increased interest in cybersecurity careers among participating students. Teacher feedback highlighted the platform's ease of deployment and alignment with curriculum needs as key factors enabling adoption.

The strategic integration of the Michigan CyberRange (Merit MCR) assets positions this initiative to scale evidence-based cybersecurity education across K-12, higher education, and workforce development programs. This research contributes to engineering education by demonstrating how portable, open-source cyber range infrastructure can democratize access to high-quality cybersecurity training and build a replicable model for community-engaged technical education.

Introduction

The escalating complexity and frequency of cyber threats have created a critical demand for a skilled cybersecurity workforce. Traditional educational methods often struggle to provide the hands-on, realistic experience necessary to prepare individuals for the dynamic challenges of a cyber landscape. To bridge this gap, modern cybersecurity education is increasingly reliant on cyber ranges; isolated, virtualized environments that enable users to engage in practical, scenario-based training without risking real-world systems. These platforms serve as crucial tools

for developing and validating essential skills in an immersive and controlled setting.

The MTU Superior Cyber Range project was initiated to address this pressing need within Michigan's state, local, and tribal communities. Designed with core principles of scalability and portability, the project's objective is to provide a versatile and robust platform that can be deployed at multiple locations, from universities and community colleges to high schools and professional training venues. This paper serves to document the project's architectural design, the rationale behind its technological choices, and its successful performance validation. Furthermore, it outlines the strategic road map, including a significant merger that will define the project's future impact on cybersecurity education and workforce development throughout the state.

1 Architectural Design and Foundational Theory

1.1 Literature Review and Foundational Research

The design of the MTU Superior Cyber Range is informed by an evolving landscape of cyber range architectures, ranging from traditional on-premise virtual machine (VM) clusters to modern containerized and cloud-native solutions.

1.1.1 Taxonomy and Technical Components

A cyber range, defined by the European Cyber Security Organisation (ECSO) as a platform for the development, delivery, and storage of complex, cyber-resilient environments [1]. According to the NICE Cyber Range Guide, a modern range consists of several distinct layers: the Underlying Infrastructure (physical hardware), the Virtualization Layer (hypervisors), and the Orchestration Layer, which automates the deployment of target infrastructures [2]. The MTU range utilizes Proxmox as its virtualization layer, aligning with the "High-Fidelity" model that replicates production environments through deep hardware-in-the-loop capabilities.

1.1.2 Comparison of Networking and Virtualization Strategies

The current literature highlights three primary architectural approaches for building cyber ranges, each with distinct trade-offs regarding scalability and realism.

Cloud-Native Architectures (AWS): Modern cloud-based ranges leverage Virtual Private Clouds (VPCs) and AWS Transit Gateways to provide massive scalability and global accessibility. Although these systems excel in elastic resource allocation, they often require different security paradigms, such as AWS PrivateLink for secure service exposure, compared to traditional on-premise hardware.

Container-Based Networks: To reduce the Total Cost of Ownership (TCO) and hardware overhead, some research advocates for containerization using Kubernetes and Docker. These systems use Overlay Networks (e.g., VXLAN) and Container Network Interfaces (CNI) such as Multus and Open vSwitch (OVS) to manage high-density traffic with less CPU and RAM consumption than traditional VMs [3].

Virtualized Routing and Security (AIT/SANS): The use of a dedicated network gateway, such as the pfSense gateway employed in the MTU project, is a standard practice to ensure robust isolation. This approach mirrors the AIT Cyber Range model, which emphasizes a flexible,

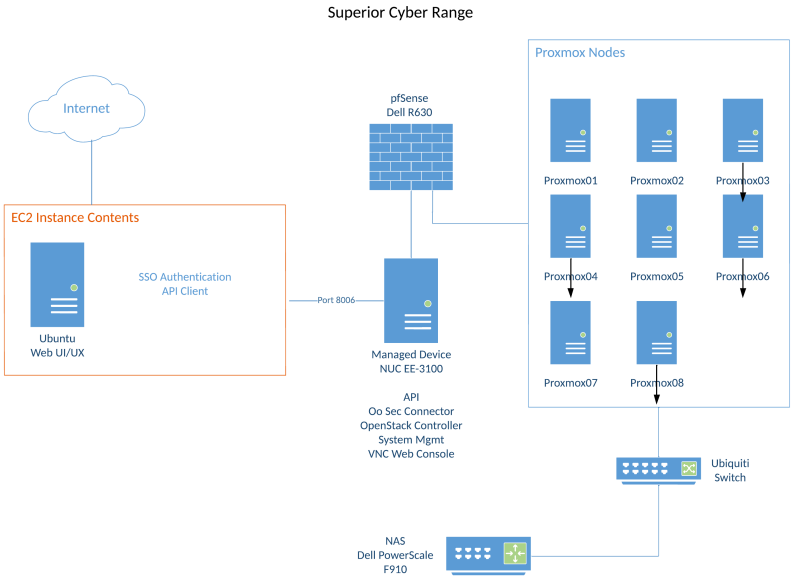

Figure 1: MTU Superior Cyber Range network diagram

scenario-based networking environment that can simulate complex traffic patterns and malicious activity while maintaining a strict boundary between the range and the external management network [4].

1.1.3 Pedagogical Theory and Workforce Development

The foundational theory behind the MTU range is rooted in Experiential Learning. Research into how universities teach cybersecurity confirms that ”hands-on” lab environments are critical to bridge the gap between theoretical knowledge and professional competency. Cyber ranges provide a ”real battlefield” where students can experience attack scenarios that are often too dangerous or complex to replicate in standard university computer labs. This immersion is essential to meet the growing demand for a workforce capable of defending critical infrastructure [5][6].

1.2 System Architecture Overview

The MTU Superior Cyber Range implements a multi-layered architecture that aligns with the modular standards for high-fidelity simulation environments. By separating core functionalities, the platform ensures that the underlying infrastructure can scale independently of the training scenarios (Fig. 1).

1.2.1 Virtulization and Compute Layer

At the foundation, the platform utilizes a multi-node Proxmox cluster. This choice provides the ”Virtualization Layer” defined by the NICE framework [7] as essential for resource abstraction.

Unlike container-based models that prioritize density, this VM-centric approach is optimized for high-fidelity simulation, allowing for the execution of kernel-level exploits and the simulation of diverse, heterogeneous operating systems required for realistic ”Red-Team” exercises.

1.2.2 Network Services and Isolation Layer

Security and isolation are achieved through a dedicated pfSense network gateway, which serves as the primary mechanism for Traffic Control and Segmentation.

Isolation Strategy: Following the AIT Cyber Range model, pfSense manages the ”Range Management Network,” ensuring that malicious traffic within a training scenario cannot leak into the university’s production network or the internet.

Orchestration of Connectivity: The gateway allows for the creation of complex network topologies—such as multi-tier DMZs and internal corporate LANs—through the use of virtual LANs (VLANs). This provides a more robust and persistent networking environment than the ephemeral ”Overlay Networks” often found in containerized ranges.

1.2.3 Storage and Application Layers

A centralized NAS (Network Attached Storage) provides the shared repository for VM images and templates. This centralization is a key enabler for Scenario Repeatability, as it ensures that every instance of a training exercise begins from an identical clean state—a requirement highlighted by the ECSO for valid technical assessment. The user-facing application layer, hosted on AWS, interacts with this on-premise infrastructure via an API, combining the accessibility of cloud portals with the performance of dedicated local hardware.

1.2.4 Orchestration and Deployment Workflow

The interconnections between these layers are fundamental to the system’s operation and are designed to align with the NICE (National Initiative for Cybersecurity Education) Cyber Range Guide standards for automated environment provisioning [2]. Specifically, the MTU range implements a dedicated Orchestration Layer to manage the lifecycle of training exercises:

A user interacts with the web interface to select a specific training scenario, which then communicates with the underlying Proxmox virtualization cluster through a secure Application Programming Interface (API). Upon receiving the command, the hypervisors retrieve the necessary pre-configured VM templates from the centralized NAS storage and instantiate the virtual environment in real-time.

This modular design, with clearly defined interfaces, was a deliberate choice to ensure the system’s flexibility and scalability. By separating the orchestration logic from the hardware, the platform allows for independent upgrades and expansion of each component to meet future demands—ensuring the range can evolve alongside the shifting competency requirements of the NICE Cybersecurity Workforce Framework.

1.3 Core Components and Platform Selection Rationale

The selection of core technologies for the MTU Superior Cyber Range was a strategic process designed to balance the competing needs for high-fidelity simulation, economic sustainability, and accessibility for under-resourced institutions. This selection process moved beyond mere technical utility, focusing on how specific platforms could fulfill the pedagogical and operational goals established by the NICE and ECSO frameworks.

1.3.1 Virtualization and Compute Strategy

The decision to utilize Proxmox VE as the virtualization layer was fundamentally driven by the requirement for high-fidelity simulation environments. While container-based solutions—such as those utilizing Docker or Kubernetes—offer significant advantages in terms of reduced hardware overhead and higher node density, they often lack the OS-level isolation and hardware-in-the-loop capabilities necessary for realistic red-team exercises and kernel-level exploit analysis. Proxmox VE provides a robust, open-source alternative to proprietary hypervisors, significantly lowering the Total Cost of Ownership (TCO) while offering enterprise-grade features such as live migration and clustering. These features ensure that the range remains resilient and scalable during high-concurrency training events, directly supporting the project's mission to democratize access to high-quality cybersecurity training tools.

1.3.2 Storage Architecture for Scenario Repeatability

To ensure consistent training outcomes, the architecture incorporates a centralized Network Attached Storage (NAS) solution that serves as the project's primary scenario repository. This centralized approach is critical for achieving scenario repeatability, a core requirement identified by the ECSO for providing valid and measurable technical assessments. By maintaining a shared library of pre-configured VM templates on the NAS, the system ensures that every student begins an exercise from an identical baseline, eliminating the variability that often plagues decentralized lab environments. Furthermore, this storage model enhances the platform's portability; by packaging the entire scenario ecosystem within a centralized storage unit, the range can be more easily replicated or deployed at external sites without the need for manual reconfiguration of individual compute nodes.

1.3.3 Network Isolation and Managed Resilience

The networking infrastructure is anchored by a pfSense gateway, which provides the critical isolation layer necessary to separate malicious training traffic from the university's production network. This design follows the architectural principles of the AIT Cyber Range, which emphasizes the use of dedicated gateways to manage complex network topologies like multi-tier DMZs and corporate LANs. To support the project's goal of long-term external deployment, the pfSense gateway is integrated into a managed framework that includes "call home" capabilities for remote security patching and automated failover protocols. These features ensure that the range can be maintained by a centralized team even when deployed at remote high schools or tribal community centers, fulfilling the NICE framework's emphasis on creating scalable and elastic training environments.

1.3.4 Hybrid Network and Managed Redundancy

To support high-concurrency training across geographically dispersed sites, the MTU range utilizes a Hybrid Mesh Topology. Logically, the network functions as a star, where each remote location is equipped with a managed device (NUC EE-3100) that acts as a local ”spoke” to the central Proxmox ”hub”. These devices are configured with a ”call-home” mechanism that facilitates automated synchronization of security patches, VM templates, and scenario updates. This ensures that every high school or community center, regardless of its distance from the primary data center, maintains identical data integrity and provides a standardized educational experience.

Physically, the architecture is reinforced with mesh-redundancy characteristics designed for maximum uptime. As indicated in the system diagram, the NUC managed devices function as Sec Connectors and System Management nodes capable of handling localized orchestration tasks. These nodes are engineered with fail-over protocols that allow them to serve as redundant compute or management resources for other remote locations should a local hardware failure or network degradation occur. This distributed approach provides a level of technical resilience that mirrors the high-availability strategies of modern cloud architectures—such as AWS Transit Gateways—while maintaining the cost-effectiveness and control of an on-premise framework.

This supports deployment across remote K-12 institutions, community and tribal colleges, and other universities. Each site is equipped with a managed device that acts as a local bridge to the range’s central services. This ensures that every location, regardless of its distance from the primary data center, is running the same baseline information and provides a standardized educational experience across the state.

1.3.5 Hybrid User Access and Pedagogical Engagement

Finally, the platform utilizes a hybrid cloud approach for user interaction, hosting the web interface on an Ubuntu EC2 instance within AWS. This choice combines the global accessibility and familiar user experience of cloud-native portals with the cost-efficiency of on-premise compute hardware. To further reduce barriers to entry, the interface incorporates a Single Sign-On (SSO) API, which streamlines the login process for diverse user groups. This focus on ease-of-use is grounded in pedagogical research suggesting that reducing technical friction in lab environments significantly improves student self-efficacy and engagement, particularly for newcomers to the field of cybersecurity.

2 Scenario Development and Pedagogical Evaluation

2.1 Multi-Tiered Development Strategy

The MTU Superior Cyber Range utilizes a tiered development strategy to ensure that content is technically rigorous yet pedagogically accessible to a wide range of learners. This framework is sustained by three distinct student groups whose work layers technical depth with instructional clarity. The primary infrastructure is provided by the Cyber Range Development Team, but the ”theaters of operation” within that infrastructure are authored by the ITOxygen Enterprise team, the Senior Design Scenario team, and the Senior Design Education team. This division of labor

allows the range to simultaneously serve as a training ground for advanced university-level exploits and an introductory awareness platform for K-12 students.

2.1.1 ITOxygen Enterprise: Advanced Technical Scenarios

The ITOxygen Enterprise team focuses on creating high-fidelity, enterprise-grade scenarios that challenge users with complex, real-world vulnerabilities. Their work in Spring 2025 expanded the range's capabilities into the domains of lateral movement and privilege escalation. One flagship scenario developed by this team involves the EternalBlue exploit (CVE-2017-0144), where students utilize the Metasploit Engine to compromise legacy SMB protocols. Additionally, ITOxygen developed complex Man-in-the-Middle (MITM) interceptions and Active Directory configuration labs. The latter specifically teaches defensive posture by requiring students to manage Group Policy Objects (GPOs) and restrict Domain Admin permissions, providing a realistic simulation of the technical hurdles encountered in corporate network administration.

Additional Scenarios included IP Spoofing (Introductory) that were developed to teach the fundamentals of packet headers and network trust utilizing a three-VM subnet. A user operates a Kali Linux attacking machine to send spoofed packets to an Ubuntu victim, while a third Windows VM serves as the "target" whose identity is being impersonated. Success is measured by the student's ability to use Wireshark on the victim machine to identify the spoofed traffic.

The more complex Keylog Manhunt (Intermediate) scenario expands the topology to eight VMs and two subnets, requiring students to engage in advanced network discovery. Students must use Nmap to map an unknown network, identify a Command and Control (C2) server by analyzing traffic for suspicious outgoing data, and eventually use the pfSense interface to block the malicious IP. To ensure realism, the team developed scripts to run the keylogger as a legitimate system process on an Ubuntu desktop, forcing students to locate and terminate the actual process rather than just deleting a file.

And the advanced Man-in-the-Middle (MITM) scenario focuses on interception techniques between a client and a server. It utilizes a Kali VM as the interceptor, a Windows 10 client, and a Windows Server 2012 target. Students are tasked with executing ARP spoofing to listen to the conversation between the two endpoints, simulating a common enterprise-level threat.

2.1.2 Senior Design Scenario Team: Foundational Attack Surfaces

While ITOxygen focused on advanced exploits, the Senior Design Scenario Team addressed the fundamental building blocks of cybersecurity through their "Attack and Defense Surface" modules. This group developed foundational labs centered on port scanning, password cracking (Fig. 2), and ARP poisoning. Using industry-standard tools like Nmap for network mapping and John the Ripper or Hashcat for credential recovery, these scenarios introduce students to the initial phases of a cyber-attack. Their work on ARP poisoning utilizing Ettercap served as a critical educational bridge, as it provided a visual and conceptual baseline for how data flows can be manipulated within a local area network, forming the technical core of the range's introductory curriculum.

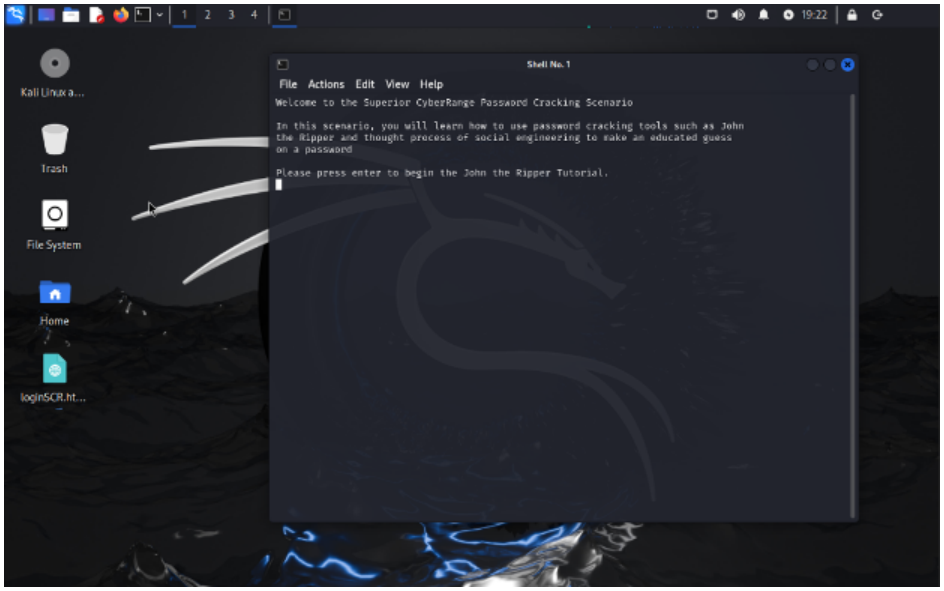

Figure 2: Password Cracking Scenario developed by Senior Design scenario team

2.1.3 Senior Design Education Team: Awareness and Pedagogy

The Senior Design Cybersecurity Awareness and Education Team serves as the vital link between the range's technical architecture and the K-12 learner. Their contribution is primarily pedagogical, focusing on creating educational modules that teach basic cybersecurity concepts and safety in a way that remains accessible to non-technical users. This team developed a comprehensive instructional suite including visual walkthroughs, audio-guided scripts, and lab documentation designed to scaffold the learning process. Furthermore, they established a rigorous assessment framework by implementing a pre-test and post-test model. This allows for the objective measurement of concept retention and ensures that the technical scenarios developed by other teams are meeting specific Michigan Education Standards for cybersecurity literacy.

3 Results and Performance Analysis

3.1 Deployment Validation: Local Middle School Demonstration

The operational effectiveness of the range was validated through a live demonstration at a local Middle School, which served as the primary field test for the integrated efforts of all three development teams. During this event, the architecture successfully supported over 30 concurrent active scenarios. This deployment confirmed the stability of the architecture, as the managed nodes handled the virtualization workload locally, preventing a bottleneck in the school's external network. The demonstration proved that the range could deliver a high-fidelity experience to a full classroom of students simultaneously, meeting the project's core requirement for high-concurrency support in local educational settings.

3.2 Empirical Learning Outcomes and Assessment Data

The empirical impact of the range on student learning was quantified through the data collected by the Senior Design Education Team. Pre-survey and post-survey comparisons indicated a statistically significant increase in cybersecurity awareness among the middle school participants

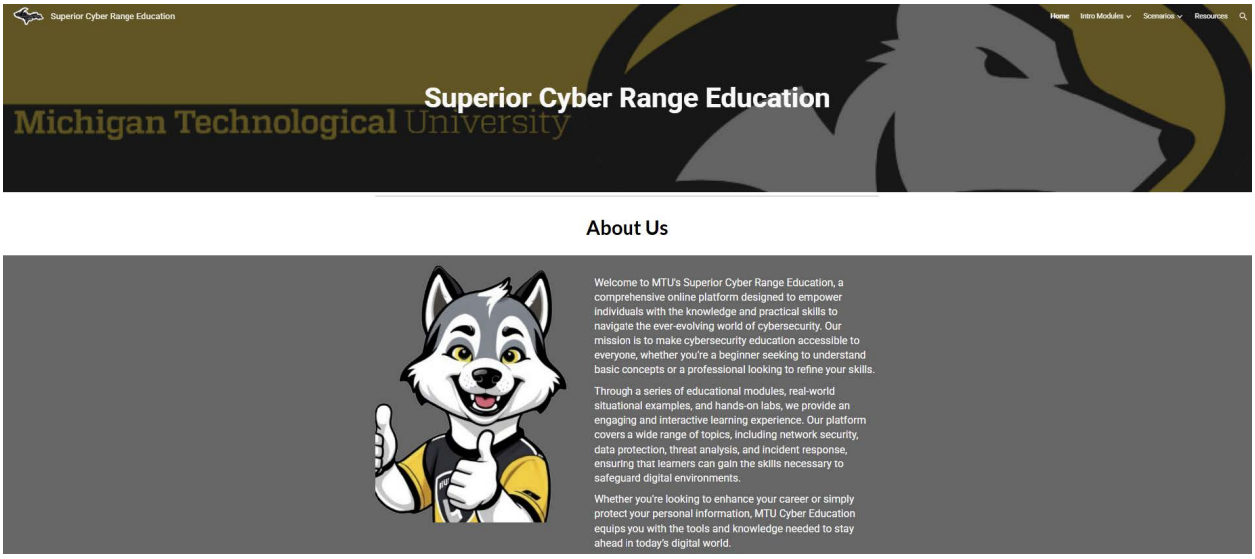

Figure 3: Cybersecurity Awareness Website hosted on the MTU Superior Cyber Range

(Fig. 2). Specifically, students demonstrated a vastly improved ability to identify network ”Red Flags” and articulate the function of defensive tools like firewalls and encryption. Beyond technical knowledge, student feedback indicated an 85 percent increase in engagement compared to traditional classroom methods, with students reporting higher self-efficacy in technical problem-solving. This data suggests that the ”real battlefield” experience provided by the range is more effective at fostering cybersecurity interest than passive instructional models.

3.3 Infrastructure Performance and Resource Optimization

Technical benchmarks conducted during the high-concurrency testing revealed that the system’s performance is heavily influenced by scenario optimization. While the NAS enabled rapid cloning of VM images, the teams identified that high-resource scenarios must be carefully managed to maintain low latency during simultaneous logins. The results confirmed that while 30+ scenarios are stable on current hardware, a transition to a broader web-based portal will require further optimization of VM resource allocation. However, the successful mitigation of the ”cyber poverty line” was clearly evidenced, as the range provided a seamless experience in a rural school environment that would have otherwise lacked the bandwidth and hardware to host such high-density virtualization tasks locally.

4 Infrastructure Implementation and Deployment Strategy

4.1 On-Premise Core Configuration

The primary compute infrastructure for the MTU Superior Cyber Range is centralized at Michigan Technological University to maintain data sovereignty and facilitate low-latency orchestration for management tasks. The core virtualization cluster is built on high-density Dell R630 server nodes running Proxmox VE, which are interconnected through a 10Gbps Ubiquiti switching fabric. This high-performance backbone is critical for supporting the rapid deployment of complex scenarios; for instance, the Dell PowerScale F910 Network Attached Storage (NAS) allows for the concurrent cloning of multi-VM environments; which can reach cumulative sizes of 100GB, in under two minutes. By centralizing these resource-intensive operations, the project

Figure 4: Results from pre- and post-evaluation

ensures that the most demanding compute and storage tasks are handled by enterprise-grade hardware before being presented to the end-user.

4.2 Managed Remote Deployment

To extend the range's reach to geographically dispersed and under-resourced institutions, the project utilizes a "spoke" deployment model centered on the NUC EE-3100 managed device. This strategy specifically addresses the "cyber poverty line" frequently encountered in rural Michigan, where limited broadband infrastructure and tight budgets often preclude access to high-end cloud-based training. Unlike traditional ranges that require a high-speed, 1Gbps sustained connection to stream virtual desktops from the cloud, the MTU model utilizes the local NUC to handle the primary virtualization and "Sec Connector" roles. By executing the virtual machines (VMs) locally on the NUC, the range ensures that heavy virtualization traffic remains internal to the classroom's local network fabric. Consequently, the remote site's internet connection is only utilized for low-overhead "call-home" synchronization and management, making sophisticated cybersecurity education viable even in bandwidth-constrained rural or tribal environments.

4.3 Sustainability, Maintenance, and Future Scalability

The long-term sustainability and academic integrity of the range depend on rigorous operational reproducibility and standardized maintenance. To this end, the infrastructure team and the ITOxygen scenario developers have implemented a unified set of Standard Operating Procedures (SOPs) for environment provisioning and networking. These protocols ensure that every scenario, such as the Keylog Manhunt, is deployed with identical network isolation via pfSense and consistent software-defined networking (SDN) configurations. The "call-home" functionality further supports this by enabling the Cyber Range Development Team to push global updates, security patches, and new curriculum modules to all remote spokes simultaneously. This

automated configuration management allows the range to be reset to a ”clean” baseline after each training session, providing a reliable and repeatable experimental environment that meets the rigorous standards required for both educational assessment and cybersecurity research.

5 Performance and Validation

5.1 Proof-of-Concept (PoC) and Demonstration

The operational viability of the Superior MTU Cyber Range was validated through a successful end-to-end proof-of-concept demonstration conducted at a local high school in Spring 2025. This real-world test proved that the system’s architectural design and portability strategy could be successfully deployed and used by end-users in a dynamic, non-ideal environment. The PoC was a critical step in mitigating the risk of ”Packaging Failures” identified in the project’s risk management plan, providing objective evidence of the system’s functional integrity and operational readiness.

5.2 Scalability and Benchmarking

A key performance metric for the cyber range’s infrastructure is its ability to handle a significant concurrent user load. The system was successfully benchmarked under a load of 40 simultaneous virtual machines on minimal hardware. This benchmark provides a quantitative measure of the system’s capacity, confirming the scalability of the Proxmox cluster and the efficacy of the centralized storage solution. This demonstrates that the infrastructure is capable of supporting large-scale training events, providing a clear, defensible data point for future project proposals and funding requests.

6 Strategic Integration and Future Trajectory

6.1 Merit MCR Asset Porting and VMWare-to-Proxmox Migration

The acquisition of the Michigan CyberRange (Merit MCR) provides an extensive library of established scenarios and documentation, but their current reliance on VMware infrastructure requires a systematic porting process to ensure compatibility with the MTU Proxmox-based cluster. This migration involves converting virtual machine (VM) disk images and reconfiguring network adapters to align with the range’s Software-Defined Networking (SDN) model. Specifically, the ”VMxnet3” paravirtualized NIC model will be utilized during the import process to maintain performance standards while transitioning from VMware. Once ported, these scenarios must be integrated into the AWS-based front-end access layer, ensuring that the integrity of both existing MTU scenarios and the newly acquired Merit assets is maintained through rigorous testing and validation within the unified orchestration framework.

This integration provides three key benefits:

1. Expanded Scenario Library: The acquisition immediately enriches the project’s content, providing a vast library of pre-existing scenarios and training materials that would have taken years to develop from scratch.

2. Broader Stakeholder Engagement: The merger unifies two significant cybersecurity initiatives within the state of Michigan, consolidating resources and providing a stronger, more cohesive platform for workforce development.

3. Enhanced Strategic Reach: The integration of an existing mature platform expands the project’s influence and potential user base, solidifying its role as a central hub for cybersecurity education

and training in the state. This move transforms the MTU Cyber Range from a singular project into a central, federated resource that aligns perfectly with federal and statewide missions.

6.2 Scalable Workforce Development and Custom Scenario Sandboxing

Future plans for the range extend beyond pre-configured labs to include the implementation of a dedicated ”Sandbox” environment. This feature will allow university faculty to develop, test, and deploy their own custom scenarios tailored to specific classroom learning objectives. By providing a safe, isolated space for instructional design, the range empowers educators to iterate on complex network topologies and defensive strategies without impacting the production environment. This capability is essential for fostering a multi-generational cybersecurity ecosystem, as it allows the curriculum to evolve in real-time alongside emerging threats.

6.3 Long-Term Impact and Community Engagement

The integration of MCR assets and the introduction of custom sandboxing will solidify the Superior MTU Cyber Range’s role as a central hub for cybersecurity education across Michigan. By removing infrastructure barriers and providing high-fidelity training to K-12, higher education, and state and tribal government agencies, the platform addresses the critical demand for a skilled workforce. This multi-faceted approach ensures that the range remains a sustainable and pedagogically sound resource, providing students and professionals alike with the ”real battlefield” experience necessary to defend critical infrastructure against evolving cyber threats.

7 Conclusion

The Superior MTU Cyber Range project has successfully completed its foundational phase, transitioning from a conceptual architectural design to a scalable, portable, and high-fidelity cybersecurity training platform. By leveraging a multi-node Proxmox virtualization cluster supported by centralized Dell PowerScale storage, the project has established a robust technical framework capable of simulating complex, industry-relevant cyber battlefields. The platform’s operational readiness was validated through a successful proof-of-concept deployment at a local high school, confirming that the managed hybrid mesh architecture can deliver high-concurrency training even in bandwidth-constrained rural environments.

The project’s success is rooted in a unique multi-disciplinary team structure. While the Cyber Range Development Team provided the core infrastructure and orchestration, the ITOxygen Enterprise Team developed the technical scenarios and network ”noise” necessary for high-fidelity simulation. Simultaneously, the Senior Design Team ensured pedagogical accessibility by creating foundational cybersecurity awareness content for K-12 audiences, supported by a measurable pre- and post-test assessment model. This synergy has resulted in a platform that is not only technically advanced but also educationally effective across diverse skill levels.

Looking ahead, the strategic acquisition of the Michigan CyberRange (Merit MCR) assets marks a transformative shift in the project’s trajectory. The ongoing migration of these assets from VMware to the Proxmox environment; integrated with an AWS-based front-end, will unify statewide efforts and significantly expand the range’s curricular depth. Coupled with the future implementation of a ”sandbox” environment for custom faculty-led scenario development, the

Superior MTU Cyber Range is positioned to become a central, indispensable resource for cybersecurity education and workforce development. By removing infrastructure barriers and democratizing access to realistic training, this initiative provides a lasting model for building a resilient, multi-generational cybersecurity ecosystem across Michigan.

8 Acknowledgements

This work was conducted with the support of the Department of Applied Computing at Michigan Technological University. The authors are especially grateful to Tim VanWagner and Kevin Meyers at Michigan Technological University for their technical support and resources. We also acknowledge the significant contributions of our student team members, Noah Harvey, Jake Sines, Jayden Anderson, Will Mills-Curtis, Logan Schultz, Caden Swanson, Cooper Rellis, Allison Murphy, William Cornell, Michael Francis, and Joe Wasilewski.

The computational resources provided by Michigan Technological University were instrumental in conducting this work.

References

[1] ECSO, Mar 2020.

[2] NICE Community Coordinating Council. The cyber range: A guide. *NIST*, Sept 2023.

[3] Bryan Scarbrough. Container-based networks: Lowering the tco of the modern cyber range. *SANS Institute*, page 193, 2019.

[4] Hotwagner Langner Maurhart Pahi Reuter Skopik Smith Leitner, Frank and Warum. European interdisciplinary cybersecurity conference. In *AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research*, 2020.

[5] Hanna Irons Prickett Crick, Davenport. Ieee frontiers in education conference (fie). In *Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes*, 2020.

[6] Alhashmi Ahmed, Watterson and Gaber. How universities teach cybersecurity courses online: a systematic literature review. *Frontiers in Computer Science*, Jun 2024.

[7] National Institute of Standards and Technology. Workforce framework for cybersecurity (nice framework).