ST. PHILIP'S TIGER CLAWS CYBER LAB AND WORKSPACE

CYBER RANGE & DATA CENTER NARRATION

RedKnight

Date Created:
March 1, 2025

PREFACE

The purpose of this narrative is to offer a comprehensive overview of the vision, development, and establishment of an interactive Information Technology (IT) sandbox, commonly known as a Cyber Range, alongside a "live" Data Center at St. Philip's College (SPC). This extensive IT infrastructure, valued at over $155 million, is strategically housed within two buildings on campus.

The primary aim of these large-scale IT deployments is to integrate the National Institute of Standards and Technology (NIST) cybersecurity framework with the standards set by the Center of Academic Excellence (CAE) in Cyber Defense, embedding these principles within the SPC Cybersecurity and Information Technology degree program. This integration enables students to transform abstract concepts related to cloud technology into practical applications, allowing them to manage live networks, create virtual environments, and engage in cyberwarfare simulations; all within a secure and controlled digital space.

By providing this hands-on experience, the Cyber Range equips students with the essential skills and knowledge needed to navigate the complexities of cybersecurity in today's rapidly evolving digital landscape. Through this innovative approach, SPC is committed to fostering the next generation of cybersecurity professionals, ensuring they are well-prepared to meet the challenges of the future.

BACKGROUND

The curriculum and pedagogy within SPC'sCybersecurity and Information Technology (CSIT) department center on bridging the gap between theory and practice.

This fundamental principle underpins the vision behind the SPC Cyber Range and the construction of the St. Artemisia Building (SAB), which houses the essential physical infrastructure. The backbone of this network is known as the CyberLab and Student Work Space (CLAWS).

The design of the SAB was intentional, aiming to facilitate the expansion of the Cyber Range into other campus buildings. The design of the St. Artemisia Bowden (SAB) was meticulously crafted to encompass all the essential elements for understanding complex network design, architecture, and management.

To facilitate this, the team implemented various access points that enable off-site locations to connect to the Cyber Range and other resources remotely.

When students visited the SAB, they were often amazed to see how easily they could access the CLAWS network through these points.

The CLAWS network has since grown to encompass the Cybersecurity Innovation Center (CIC), evolving the original Cyber Range concept into a more abstract understanding of cloud technologies. The SPC data center, referred to as the Cloud on the Ground (COTG), provides the necessary resources to manage both the CLAWS network and the CIC enterprise network. This setup not only supports local network management for the SPC IT curriculum but also opens avenues for revenue-generating opportunities for the college by leasing space on the COTG and offering time on the Cyber Range.

This successful integration effectively bridged the gap between theoretical knowledge and practical application, allowing students to engage with abstract concepts like Virtual Local Area Networks (VLANs) and cloud technology in a tangible way. This experience served as the inspiration for the Cloud on the Ground (COTG) concept, scaled up to a more extensive infrastructure. The SPC datacenter, which houses ten cabinets equipped with three inline coolers and a hot aisle containment system, further supports this vision.

ARCHITECTURAL DESIGN CONSIDERATIONS

There is a large and widening gap between college graduates in IT-based degree programs and the base requirements of the current job market. Not only is demand for system and network engineering and cybersecurity professionals substantially outpacing workforce creation according to a research paper conducted by the Cybersecurity Workforce Data Initiative and the National Science Foundation1, but there is an additional widening gap between the qualifications of recent college graduates and median job requirements for cybersecurity industry jobs. To a large degree, this gap is easily solved through practical experience, but the elevated requirements create a barrier to entry for the labor pool and thus an obstruction to gaining that needed experience.

At inception, the CLAWS environment embraced several key objectives as foundational elements for the architecture. The first of these was a need to overcome the gap between new workforce and available jobs. Specifically, CLAWS was designed to provide practical experience that directly matches the experience required by employers. To accomplish this, CLAWS employed what was termed the "pod concept" and general modularity throughout the system. Pods are composed of two student workstations with VMware Desktop installed, one Cisco network switch, one Cisco network router, and one Dell server running VMware Essentials.

Each pod allows a pair of students to create a virtual environment modeling a small business. More importantly, the pods are a practical demonstration to students of how a very similar test environment could be created at for personal use with very little capital outlay. Pods were designed to be combined logically in order to allow multiple pairs of students to create a more complex environment of many small businesses networked to model a regional business.

These virtualized environments can then be intentionally compromised in simulated attacks, generating real indications of compromise for ingest by Security Information and Event Management (SIEM) systems.

The increased realism of event alerting is a benefit but pales next to the more substantive benefit of the compromised live environment. Students are not limited to simply recognizing the malicious activity through events but are able also able to log into compromised systems, conduct troubleshooting, isolation, and forensic analysis in very true-to-life scenarios.

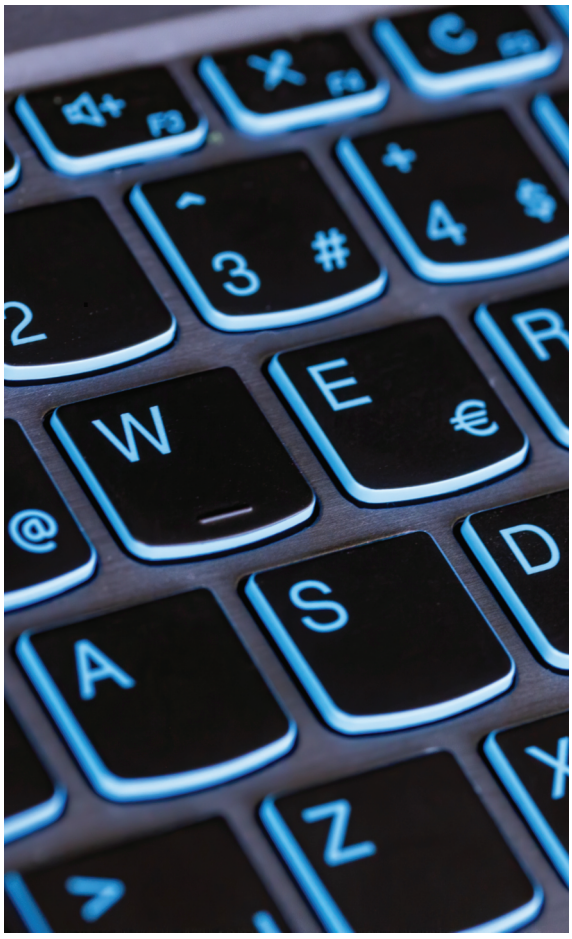
The second design consideration originated with an awareness that many small businesses supporting Department of Defense cyber operations need test environments for their own tools and payloads. The modularity of CLAWS was designed to allow maximum flexibility in isolating traffic and operations between elements of the range. This provides the capability to "carve off" elements of the larger range for use by companies or to support other research efforts.

The support of Defense industry small businesses required the environment also implement security controls as described in the NIST 800-series publications. Specifically, the controls cited in NIST 800-53 were addressed so that organizations required to implement the Risk Management Framework (RMF) as described by NIST 800-37 could utilize resources from the CLAWS environment with minimal delay for approval.

This modularity also has the tangential benefit of CLAWS being ideally suited for supporting small start-up companies. Students of the sponsoring institution are expected to be given priority in access to the environment, but CLAWS continues to expand with additional funding. The expanded environment is capable of dynamically supporting an increasing number of start-up projects and is particularly suited as a testing ground for information security applications and monitoring tools.

FUNDAMENTAL OF NETWORKING

The second floor of the SAB features two classrooms dedicated to the fundamentals of networking. These rooms are thoughtfully designed with a setup of five hardwired computers connected to a rack of equipment, which includes a switch, router, and firewall. The courses held in these classrooms lay the groundwork for understanding complex network designs. Utilizing the Open Systems Interconnection (OSI) model as a conceptual framework, students learn to implement effective network communication.



Initially, students are tasked with establishing communication between the computers using the racked equipment. As they master this, they learn to configure the system for broader communication across all computers in the row, gradually limiting interactions between them to deepen their understanding. Once these foundational concepts are grasped, the focus expands to utilizing multiple routers, switches, and firewalls throughout the room.

To further enhance their comprehension, students are encouraged to think on a larger scale—conceptualizing one row as an entire state and each computer as a city. This analogy illustrates that the same types of equipment, protocols, and configurations apply to larger cross-country networks. Ultimately, while the complexity and scope may differ, the fundamental principles of networking remain constant.

VIRTUALIZATION, VIRTUAL LOCAL AREA NETWORKS(VLANS)& OPERATING SYSTEMS

These classrooms, dedicated to operating systems, virtualization, and VLAN configuration, are integral to the educational framework of the SPC Cyber Range. By emphasizing Virtual Local Area Networks (VLANs), students develop essential skills in managing and optimizing network resources effectively. The integration of VLANs with Virtual Machines (VMs) enables the creation of diverse networks that replicate real-world scenarios, providing students with a practical context for their learning.

This hands-on approach allows students to actively monitor network traffic and analyze critical indicators, equipping them to identify and respond to cyberattacks with confidence. Through simulations and practical exercises, they gain invaluable experience in troubleshooting and mitigating security threats, thereby solidifying their understanding of network security principles.

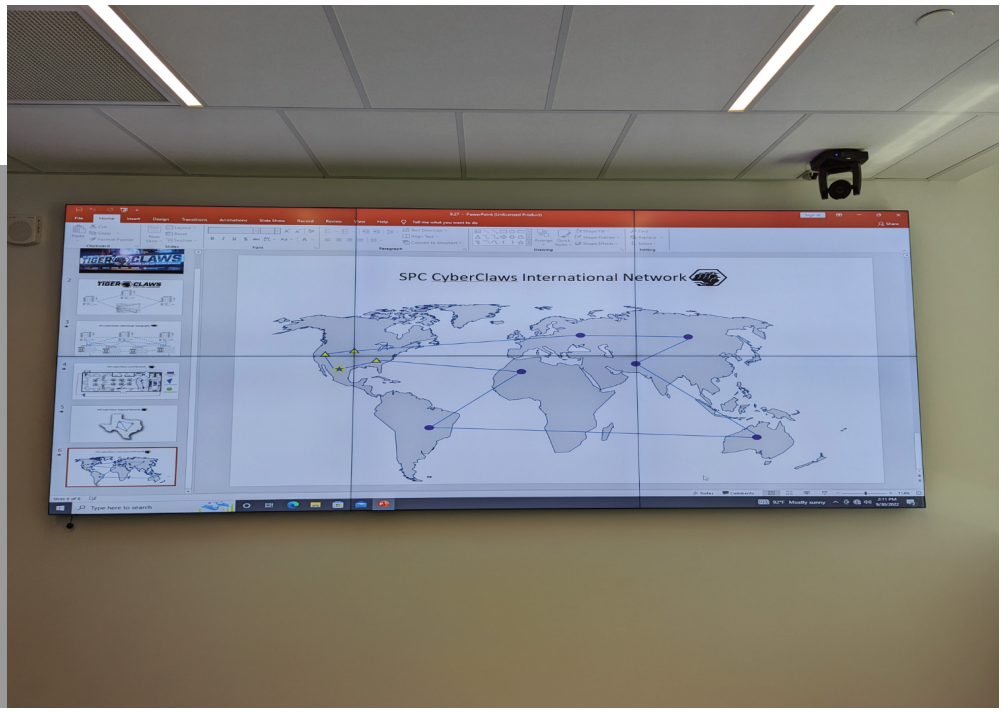
This practical training not only enhances their technical expertise but also prepares them to navigate the complexities and challenges of cybersecurity in an ever-evolving digital landscape. By fostering a robust understanding of both theoretical concepts and real-world applications, these classrooms play a pivotal role in shaping the next generation of cybersecurity professionals.

CYBERLAB AND STUDENT WORKSTATIONS (CLAWS) AND CYBER RANGE

The areas mentioned are crucial not only for understanding complex networks, infrastructure, and virtualization but also for forming the foundational elements of the CLAWS network and the Cyber Range. As a sophisticated IT setup, CLAWS, along with the various virtual environments deployed on the Cyber Range, serves two key purposes. First, it enables students to observe how a comprehensive environment is designed, configured, and installed. Second, it facilitates the practical application of cybersecurity tools, ranging from identifying vulnerabilities in an open network to utilizing monitoring tools and addressing more complex exploitations.

The Cyber Range at SPC is an invaluable resource for anyone looking to enhance their cybersecurity skills. It offers a safe, controlled environment for training, testing, and refining abilities, effectively blending virtualized settings with real-world applications. Additionally, the Cyber Range is highly customizable and scalable, allowing it to adapt to diverse learning needs while considering security requirements in its design and construction.

CYBERSECURITY INNOVATIONS CENTER (CIC)



The vision behind the Cybersecurity Innovations Center (CIC) was to provide a more hands-on experience with IT networking equipment and cybersecurity hardware. The primary goal was to transform abstract concepts into practical applications that enhance understanding. The CIC datacenter, known as the Cloud on the Ground (COTG), successfully achieves this objective while extending the capabilities of the Cyber Range across the campus.

The COTG allows students to engage in live datacenter management within a real-world Security Operations Center (SOC), providing invaluable experience in the rapidly evolving field of cloud computing and technology. Through this setup, students learn about cloud architecture, design, and various cloud services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

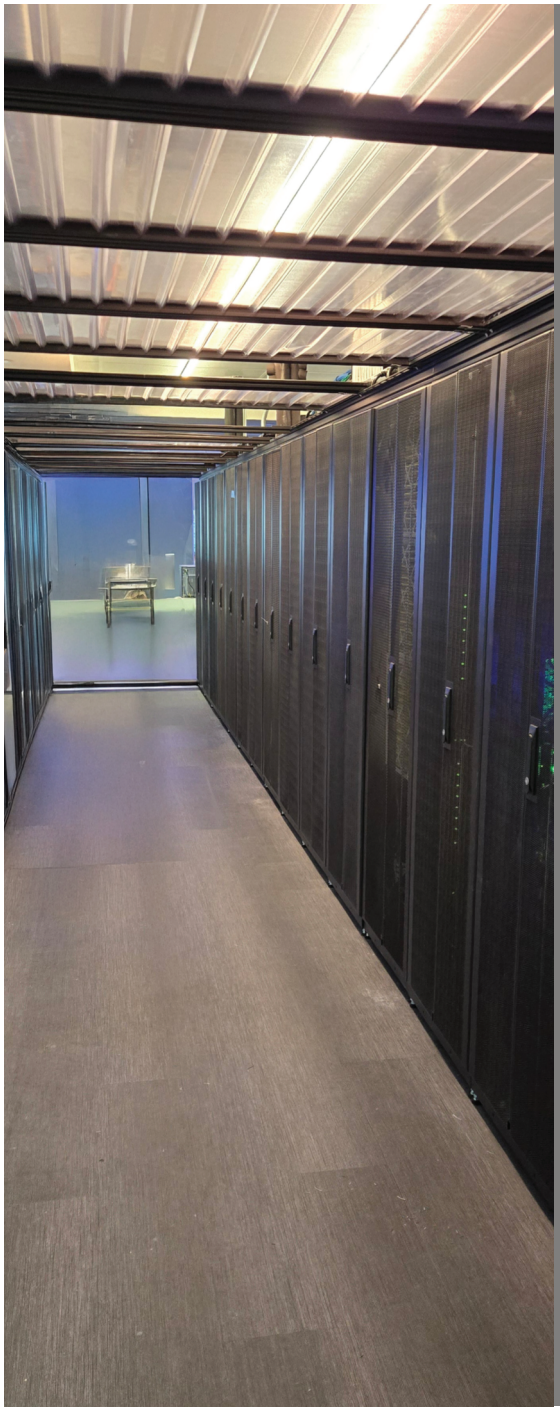
Cloud computing is fundamentally transforming business operations by providing organizations with enhanced flexibility, scalability, and cost savings. By leveraging cloud technologies, businesses can quickly adapt to changing market demands, scale their resources up or down as needed, and reduce the overhead costs associated with traditional IT infrastructure.

Currently, the delivery of these cloud services is primarily confined to the academic environment, where students gain valuable experience and skills. However, there is a forward-thinking vision to expand these offerings into revenue-generating opportunities for the college. This initiative aims to create partnerships with local businesses and organizations, allowing them to utilize the college's cloud infrastructure for their own operations while providing students with real-world projects and practical experience.

By transforming the CIC and COTG into a hub for cloud services, the college can further enrich the educational experience for its students. They would not only engage in simulated learning but also participate in live projects that impact the community. This approach not only enhances student learning but also positions the college as a key player in the regional tech ecosystem, fostering innovation and collaboration.

The vision of expanding cloud service delivery aligns with the college's mission to prepare students for the workforce, equipping them with the skills and experience necessary to thrive in an increasingly digital economy. By blending education with practical application, the college can ensure that its graduates are well-prepared to meet the challenges and opportunities presented by the evolving landscape of cloud computing and cybersecurity.

ST. ARTEMISIA BOWDEN (SAB) AND CYBERSECURITY INNOVATION CENTER (CIC)

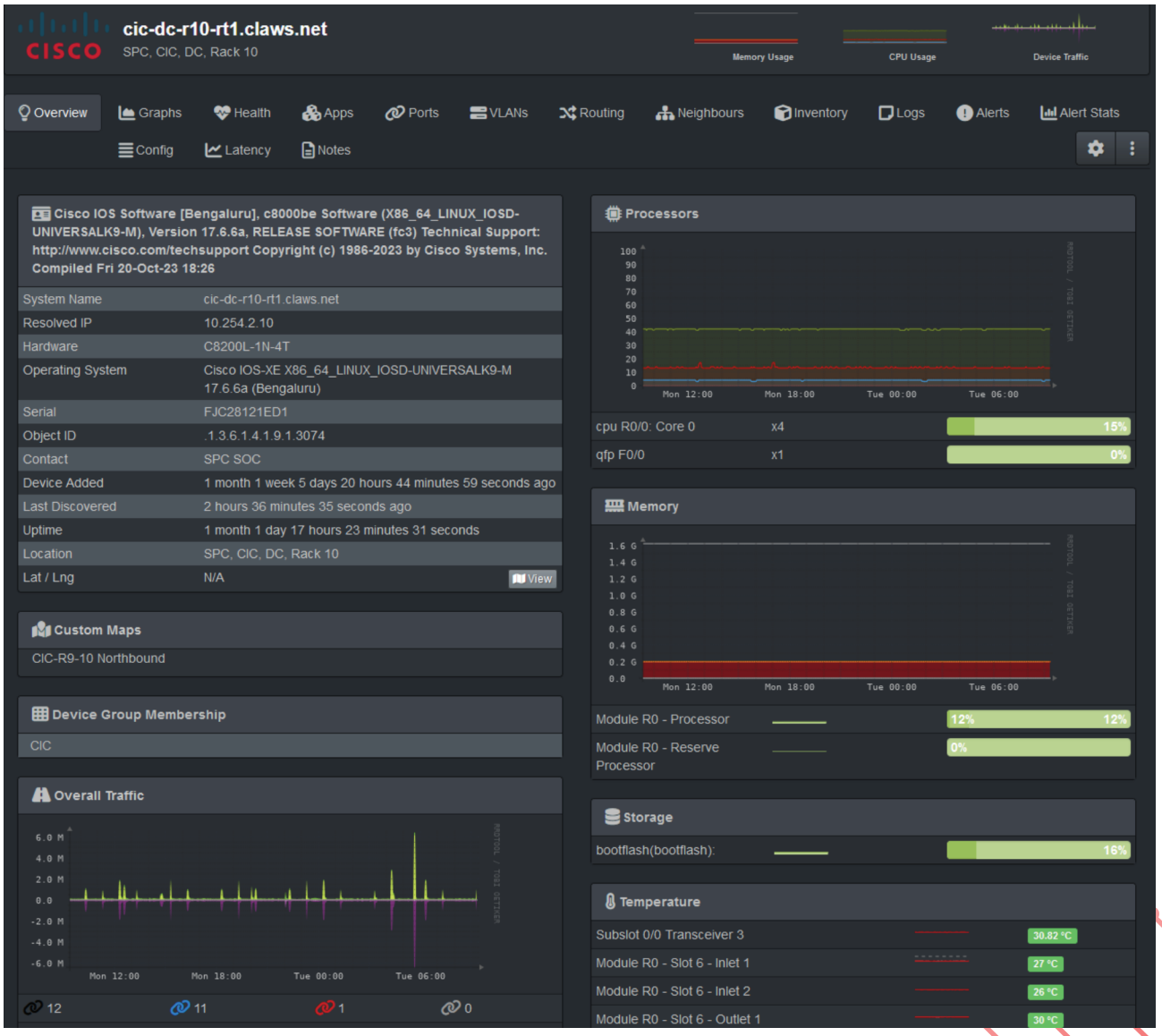


While the integration of the SAB Cyber Range and the CIC Cloud on the Ground is still evolving, the concepts and hands-on experiences related to network monitoring and cybersecurity are proving to be invaluable for students. The establishment of the Security Operations Center (SOC) and the disaster recovery simulation room within the CIC significantly enriches this educational landscape, providing students with essential insights into the critical role of effective communication in cybersecurity.

These advanced facilities not only offer practical training but also present real-world scenarios that challenge students to understand the complexities and organizational breadth of cybersecurity. By engaging in simulated incident responses and disaster recovery exercises, students learn to collaborate effectively, share information promptly, and develop strategic solutions under pressure. This experiential learning cultivates the ability to think critically and adapt to rapidly changing circumstances, essential skills in the dynamic field of cybersecurity.

Moreover, the SOC environment immerses students in the day-to-day operations of cybersecurity management, allowing them to interact with various tools and technologies used in the industry. They gain firsthand experience in monitoring network activity, identifying potential threats, and responding to security incidents—all vital components of a successful cybersecurity strategy.

By equipping students with these competencies, the CIC and its integrated facilities ensure that graduates are not only technically proficient but also adept at navigating the complexities of cybersecurity within organizational contexts. This comprehensive approach prepares students to meet the challenges of the evolving cyber landscape, fostering a new generation of professionals ready to make meaningful contributions to the field.



CLOSING THOUGHTS

The development of the Cyber Range and the Cybersecurity Innovations Center (CIC) at St. Philip's College represents a significant leap forward in bridging the gap between theoretical knowledge and practical application in the field of cybersecurity. By integrating advanced IT infrastructure within a controlled environment, students gain hands-on experience that enhances their understanding of complex network systems, cloud technologies, and cybersecurity protocols. This innovative approach not only prepares students for the evolving demands of the cybersecurity landscape but also positions SPC as a leader in cybersecurity education. As technology continues to advance, the initiatives undertaken in the St. Artemisia Building (SAB) and the Cybersecurity Innovations Center (CIC) will provide students with the skills \necessary to excel in their careers, while also creating potential revenue-generating opportunities for the college.

This comprehensive educational framework fosters a new generation of cybersecurity professionals equipped to tackle the challenges of the digital age, reinforcing SPC's commitment to excellence in academic and practical training.