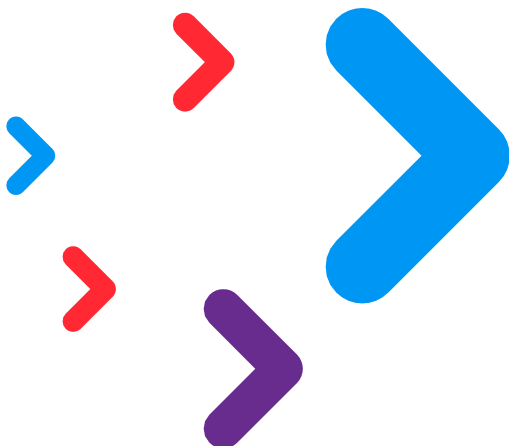




Cyberbit for Columbus State University



Case Study





The Customer: Columbus State University

Columbus State University (CSU) is a public university in Columbus, Georgia and is part of the University System of Georgia. Located just 100 miles southwest of Atlanta, CSU enrolls over 7,000 students each year and offers more than 90 undergraduate and graduate degree programs. CSU will benefit from the recent passage of Senator Warnock's jobs and competition bill, which secured generous funding for STEM education, especially at historically black colleges and universities (HCBUs).

The Challenge: To grow regional and national cybersecurity talent that will help address the skills shortage.

Dubbed the "Tech Capital of the South", Georgia's financial services and technology industries provide most of the economic growth in the state. In the past year, demand for cyber security professionals in the State of Georgia has increased significantly. With over 25,000 open positions, Georgia is now eighth in the nation for new cybersecurity job openings. Columbus State University wanted to establish a cybersecurity training program that could serve the local community, grow cybersecurity talent in the region, and help address the local and national skills shortage.

The most optimal way to achieve this was by establishing a cybersecurity program that could produce graduates who are work ready the minute they enter the workforce, provide skill development and upskilling for cybersecurity professionals already in the field, reskill veterans, first responders and other professionals, and foster recruitment and development of underrepresented demographics.

Georgia's Cybersecurity Job Market



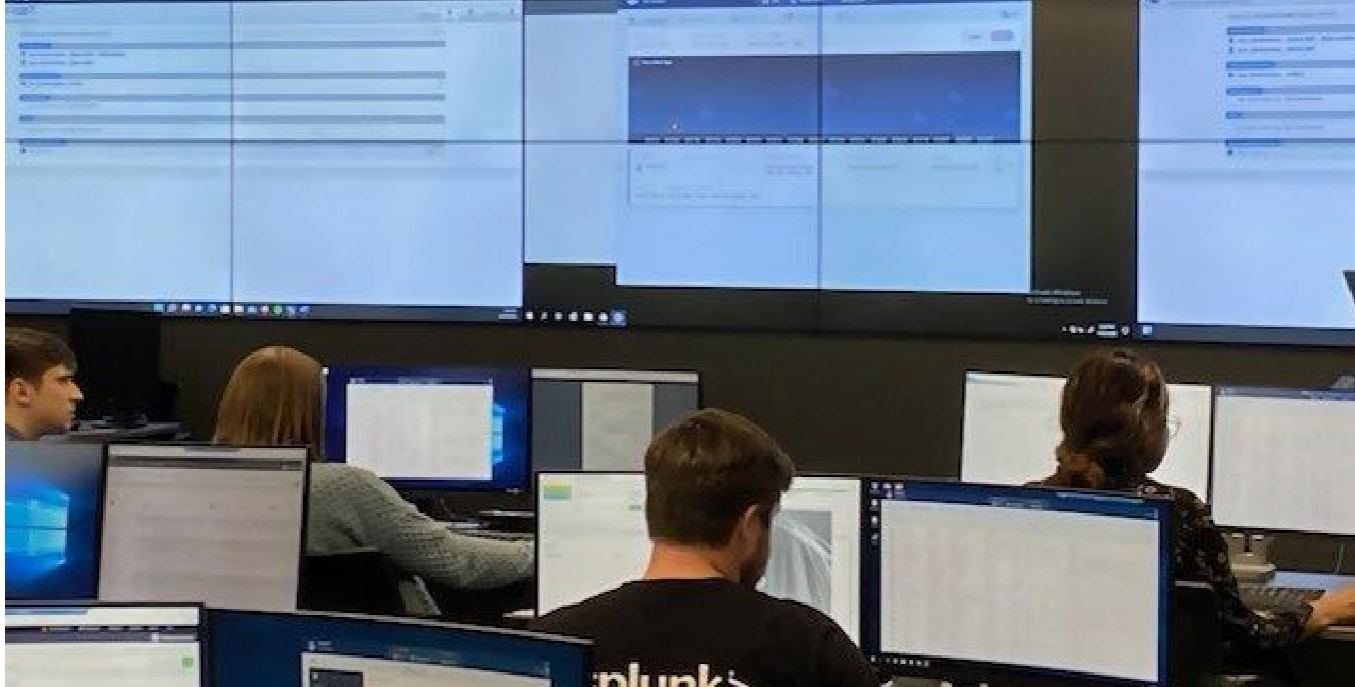
Total Cybersecurity
Job Openings

25,082

Total Employed
Cybersecurity
Workforce

35,986

Source: CyberSeek.org



The Solution: The Cyberbit Range

Columbus State University opened the TSYS Center for Cybersecurity as part of a \$2.5 million project. Built with the help of a \$5 million gift from Total System Services Inc (TSYS), a Global Payments company, the center includes the Cyberbit cyber range.

The Cyberbit range has been integrated into three CSU cyber range programs, providing hyper-realistic simulated attack experiences to CSU students and professionals. Cyberbit's cyber range was chosen by CSU as the best technology for preparing the type of qualified, high-performing cybersecurity professionals needed to help address the critical skills shortage.

Recruiters from 80 major companies interviewed 60 students from CSU's Nexus-R program and said they were surprised and impressed with the students' knowledge and skills. Nearly all of these students were offered positions by these companies.

Delivering experiential, hands-on training, the range is a "live-fire" range, allowing students to experience and practice in hyper-realistic environments that include enterprise grade networks, commercial security tools, and simulations of the real-world cyber-attacks they'll encounter on the job such as ransomware, supply chain, web defacement attacks, and others.

CSU makes the range available to industry professionals as well as its students, helping them move up in their current careers or transition to new careers in cybersecurity. Corporations also send their SOC teams for workshops using the Cyberbit range to learn the techniques and skills needed to defend against today's sophisticated cyber-attacks. CSU also provides individual scenario training upon request.

CSU integrates the Cyberbit cyber range into three of its cybersecurity programs:

1. The Nexus Program offers a one-year certificate program as well as a two-year complete cybersecurity degree program. Upon completion and passage of the one-year program students receive **CompTIA Network Plus, Network Security, or IT Fundamentals certificates**.
2. The **Nexus-Range (Nexus-R) Defender (Blue Team) Program** is a **6-week program** for professionals who already possess networking or cybersecurity experience and are looking to move into a cybersecurity position. This course covers principles in cyber and information security and a range of topics such as the latest threat vectors, vulnerabilities, detection, forensics, recovery, and more. Participants of this course will gain hands-on experience on the Cyberbit range in an immersive environment mirroring real-world cyber-attacks, corporate grade networks, and powerful commercial security tools.
3. The Nexus-Range (Nexus-R) Invader (Red Team) Program is a 6-week program that focuses on industrial security tools used in offensive security operations, including kill chain and MITRE ATT&CK frameworks. This program is also directed at professionals who are moving into cybersecurity positions and already possess requisite networking and information security skills. Course participants will gain hands-on experience in live-fire attack scenarios on the Cyberbit range, developing their skills in networks, protocols, web applications, penetration testing and more.

Workshops

CSU also offers 3 and 4-day training workshops that are tailored to the expertise level of the participants. After the workshop, participants engage in real-world cyber-attack scenarios on the Cyberbit range. Workshops are offered for training SOC team tier 1, tier 2, and tier 3 analysts.

Tier 1 SOC

Trainees will be introduced to operations security (OPSEC) including the basics of Windows, Linux, and network forensics. Key concepts and tools include systems monitoring, commercial SIEM (Splunk & QRadar), firewall, and more.

Trainees

- Personnel moving into SOC roles
- Tier 1 SOC Analyst

Prerequisites

- Nexus R Essentials Completion or
- 2+ years cyber security experience.

I. Nexus Range (Nexus R) Essentials Track

Blue Team Cyber Defense

- Participants will learn the principles of cyber and information security.
- Topics covered include Threats, Attacks and Vulnerabilities, Securing Data and Applications, Incident Response, Forensics, and Recovery.
- Hands on with the required Cyber Range tools and techniques to stop advanced cyber attacks.
- IT and network background knowledge are prerequisites.
- Offering mode: in person, hybrid, and online.
- 6 week program.

II. Nexus Range (Nexus R) Essentials Track

Red Team (Ethical hacking)

- Participants will gain foundational skills on computer networks, protocols, web applications, and the most important technical aspects of penetration testing.
- Provide hands on experience with the latest hacking tools, techniques, and methodologies to lawfully test an organization's vulnerabilities.
- This course covers different phases from information gathering through footprinting, as well as scanning and vulnerability.
- IT and network background knowledge are prerequisites.
- Offering mode: in person, hybrid, and online.
- 6 week program.

Assessments & Credential

- Successful completion through 75% or higher
- total grade in scenario reports.
- Trainees will receive digital badge credential via Accredible.

The Benefits: Helps meet industry demand for work-ready cybersecurity professionals, positions CSU as a technology hub for Georgia

Since launching its cybersecurity program with the Cyberbit range, CSU has been able to offer the type of cybersecurity training that creates workforce-ready graduates and cyber defense experts, equipped with critical hands-on experience in dealing with cyber-attacks, the type of real-world experience requested by employers.

The quality of CSU graduates from these programs is very high with most receiving apprenticeships and internships from well-known local companies such as Global Payment, Aflac, Synovus, and others. Approximately 95% of interns and apprentices then go on to receive job offers from these companies after completing their internships.

“Currently, the most significant factors behind data breaches are the lack of proper training and the lack of highly skilled cybersecurity professionals. The Cyber Range at CSU helps close that gap, by allowing us (students) the ability to train in real-world scenarios we are able to transform our theoretical classroom-based discussions into hands-on practical cybersecurity training that is followed up with a performance-based evaluation. Additionally, to building technical skills we also gain soft skills in the form of collaboration by effectively communicating simultaneous tasks in a timely matter as well as having the emotional IQ to cover down in the event a teammate is in distress. Resulting in a stronger foundation when we start our cybersecurity careers.”

Tyvon Cruz – Nexus student, Cohort 4

“The Cyber Range offers a real-world tactical sandbox environment that allows us to engage with technologies that are used by the industry while allowing us to learn and develop our capabilities. The effective measure is shown by our ability to communicate beyond a textbook definition of a problem and work to a solution as a team. This valuable training system better prepares us for the battle sphere and evolving threats possessed by adversaries around the globe.”

Cabello, Fernando – Nexus student

The state-of-the-art range helps enrich students’ academic experience, strengthen industry partnerships, generate interest in CSU’s cybersecurity program, and expand the school’s reach to underrepresented demographics.



“We provide a variety of learning and training programs for students and professionals who are moving into cybersecurity roles. With a controlled, interactive environment such as Cyberbit’s cyber range, we offer the latest technology and training methods in cyber defense and penetration testing.”

Ehab Bedir,

Cyber Range Network and Computer Systems Administrator of the TSYS Center for Cybersecurity

About Cyberbit

Cyberbit provides hands-on cybersecurity education and training and addresses the global cybersecurity skill gap through its world-leading cyber range platform. Colleges and universities use the Cyberbit range to increase student enrollment and retention, train industry organizations, and position their institution as regional cybersecurity hubs by providing simulation-based learning and training. The Cyberbit platform delivers a hyper-realistic experience that immerses learners in a virtual security operations center (SOC), where they use real-world security tools to respond to real-world, simulated cyberattacks. As a result, it prepares students for their careers in cybersecurity from day-one after their graduation and reduces the need to learn on the job. Cyberbit delivers over 1,000,000 training hours annually across 5 continents. Customers include Fortune 500 companies, MSSPs, system integrators, higher education institutions and governments. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia.

US

3571 Far West Blvd. #168 Austin, TX 78731 | Tel: +1 512 676 8731

UK

103 Kingsway London WC2B 6QX | Tel: +44 (0) 2032 069400

Singapore

Temasek Avenue Centennial Tower, #21-23 Singapore 039190 Tel: +65 6679 5771

Israel

22 Zarchin St. Ra'anana 4310602 Israel | Tel: +972 (0) 9.779.9831

Germany

Mies-van-der-Rohe-Str. 880807 Munich Germany | Tel: +49-89-215416-22