CYBER COLOSSEUM BY RedKnight

A STANDARDIZED, REPEATABLE CYBER RANGE
FOR REAL WORLD CYBER THREAT MANAGEMENT

WWW.NATUV.COM/CYBER-COLOSSEUM

COLOSSEUM@NATUV.COM
(405) 724-3193

What is a Cyber Colosseum ?

Is a production-ready initiative where students and professionals learn cybersecurity the same way Formula 1 drivers learn to race by practicing in a realistic simulator, not just reading textbooks. Instead of learning cyber concepts solely in classrooms, students and participants train in a live, controlled environment that which real-world cyberattacks and defenses.

Developed and operated in collaboration with industry pioneers like National Security Agency (NSA), Dell Technologies, CrowdStrike, and Cisco, we ensure the infrastructure, tooling, and threat models reflect what students will encounter in live environments.

The Problem

- Cyber graduates leave with theory, not operational experience
- Employers struggle to find job-ready cyber defenders
- Universities need differentiation, placement outcomes, and workforce relevance

Solution

Red Knight's Cyber Colosseum immerses students in realistic attack and defense scenarios, enabling hands-on experience with modern adversaries, tools, and decision-making under pressure.

Competitive Cyber Defense at Scale

- In addition to live red-team vs blue-team cyber exercises, the Cyber Colosseum incorporates ethical development and use of Artificial Intelligence (A.I.) alongside machine learning for better cognitive cyber defense.
- Students actively work with:
  - A.I.-assisted ethical hacking tools to identify vulnerabilities faster and more accurately
  - Machine learning models trained to detect anomalies, intrusion patterns, and zero-day behaviors
  - Automated threat classification and response simulations used by enterprise and government security operations centers (SOCs)

Credentialing: Upon successful completion, students receive a formal Cyber Range Colosseum of Completion, validating hands-on experience in the areas of cyber offense and defense operations, A.I.-assisted security tooling and realworld incident response scenarios.

- This certificate is designed to be employer recognizable and complements academic coursework and industry certifications, increasing talent visibility for government, defense, and private-sector employers

Dual-Use Facility: Cyber + eSports

Designed with high-performance GPU workstations, the facility can seamlessly function as both:

- A cyber range for training and operations
- An eSports arena for competitive gaming and events
- Maximizing student engagement and adding one of the fastest growing sports to the universities athletic calendar

Beyond Training: A Community Cyber Asset

- The facility and its students can also provide real services, including:
  - Cybersecurity monitoring for the university and neighboring communities Hosting and managed IT services for municipalities, non-profits, and small businesses
  - Workforce-in-practice experience that produces job-ready graduates

How the Cyber Colosseum Is Used

- Course labs and applied learning
- Capstone simulations and team exercises
- Intercollegiate attack and defense competitions and scenarios
- Faculty-led and student-driven scenarios

SolutionNational Readiness & Strategic Support

- Beta and Phase I locations are actively installed and progressing at Saint Philips College in San Antonio, Texas.
- In the event of a significant cyber incident or national cyber emergency, the facility can transition into an active support node, augmenting defense partners such as Tinker Air Force Base and participating corporate sponsors

Why This Matters (At a Glance)

- • “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” GlobeNewswire, 18 Nov. 2020.
- https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html
- • Security Magazine. (2023). 71% of organizations are impacted by cybersecurity skills shortage.
- https://www.securitymagazine.com/articles/99865-71-of-organizations-are-impacted-by-cybersecurity-skills-shortage
- • Alder, S. (2026). Ransomware attacks increased 58% in 2025. HIPAA Journal.
- https://www.hipaajournal.com/ransomware-attacks-increased-58-percent-2025/
- • 70% of organizations say hands-on training is the most effective way to build real-world cyber skills
- Source: ISC2 Cybersecurity Workforce Study
- • Teams that regularly conduct hands-on exercises (e.g., simulations, tabletop, labs) improve incident response times by up to 50%
- Source: IBM Security Cost of a Data Breach Report

Who Is Behind This

RedKnight brings leadership experience rooted in the U.S. national security ecosystem, with backgrounds aligned to NSA and CIA operational environments, shaping the realism and rigor of all cyber scenarios.

Natuv is a U.S.-based, Native American owned technology company supporting federal, defense, and critical-infrastructure programs, with experience operating secure and mission-critical systems.

See It in Action →

Contact Us

https://www.natuv.com/cyber-colosseum
colosseum@natuv.com
C: (405) 724-3193

RedKnight | NATUV