NATIONAL SCIENCE FOUNDATION (NSF) GRANT PROPOSAL

Directorate for STEM Education (EDU) / Division of Undergraduate Education (DUE)

Program Directorate:	Directorate for STEM Education (EDU) / Division of Undergraduate Education (DUE)
Program Solicitation:	Improving Undergraduate STEM Education: Education and Human Resources (IUSE: EHR)
Project Title:	Scaling Adaptive Cybersecurity Education: Integrating Automated Threat-Simulation Labs into Undergraduate Computer Science Curricula
Principal Investigator:	Regional Technical Systems Alliance
Requested Funding:	$350,000
Project Duration:	36 Months (September 1, 2027 – August 31, 2030)

1: PROJECT SUMMARY

Intellectual Merit
The project investigates the pedagogical efficacy of integrating real-time, automated threat-simulation sandboxes into undergraduate cybersecurity and computer science courses. Traditional cybersecurity education relies heavily on static textbook scenarios and delayed assignment grading, failing to prepare students for dynamic, evolving threat landscapes. This project develops CyberSim-AI, an open-source, containerized learning environment driven by automated AI agents that dynamically generate unique vulnerabilities and attack vectors tailored to a student's current skill level. The research evaluates how adaptive, real-time threat feedback impacts student algorithmic problem-solving speed, threat-hunting proficiency, and long-term security mindset.

Broader Impacts
The project addresses the critical national shortage of qualified cybersecurity professionals by expanding equitable access to high-fidelity training tools at community colleges and minority-serving institutions. By lowering the infrastructure barrier required to host complex security labs, the project will equip 40 undergraduate educators with turnkey cloud-based modules, reaching over 600 students annually. All software frameworks, AI generation scripts, and instructional rubrics will be published under open-source licenses to foster nationwide curriculum modernization.

2. PROJECT DESCRIPTION & NARRATIVE

2.1 Introduction and Rationale

Modern digital infrastructure faces unprecedented security threats, yet undergraduate computer science programs struggle to provide realistic, hands-on defensive training due to infrastructure costs and static lab designs. Students learn defensive coding in isolated environments where exploits are predictable and artificial.

This project establishes the Adaptive Threat-Simulation Framework, shifting education from passive security theory to active, automated red-team vs. blue-team simulation. By embedding lightweight AI agents into student coding environments, the platform dynamically generates realistic network anomalies, privilege escalation attempts, and malware propagation patterns that students must identify and remediate in real-time.

2.2 Research Objectives & Hypotheses

Objective 1: Engineer and deploy the CyberSim-AI orchestration engine across 4 pilot undergraduate institutions.

Objective 2: Measure the quantitative impact of automated adaptive difficulty scaling on student code vulnerability reduction rates.

Objective 3: Establish an open-access repository of automated security challenges mapped to standard ACM/IEEE cybersecurity curriculum guidelines.

Research Hypothesis: Students utilizing the AI-driven adaptive simulation environment will exhibit a 30% faster incident response time and a 40% lower recurrence rate of common security vulnerabilities (e.g., SQL injection, buffer overflows) compared to control groups using static lab manuals.

3. INTELLECTUAL MERIT: RESEARCH & PEDAGOGICAL INNOVATION

3.1 Framework Architecture & Feedback Loops

The core innovation lies in the Dynamic Difficulty Adjustment (DDA) Engine, which analyzes student keystrokes, syntax errors, and patch attempts to adjust the sophistication of simulated network intrusions.

Below is a structured overview of the multi-tier simulation architecture:

Tier	Simulation Level	AI Agent Behavior	Target Student Skill
Tier 1: Foundation	Static Network Logs	Flags basic anomalous traffic patterns	Log parsing & Regex filtering
Tier 2: Intermediate	Automated Port Scanning	Simulates active reconnaissance and brute-force	Firewall configuration & patch management
Tier 3: Advanced	Polymorphic Malware Simulation	Mutates attack signatures dynamically	Real-time threat hunting & heuristic analysis

3.2 Quantitative Impact Metrics (Projected Growth Across Cohorts)

STUDENT PROFICIENCY & VULNERABILITY MITIGATION TRAJECTORY

Threat Identification Accuracy	
Cohort 1 Baseline: 52%	**Cohort 2 AI-Assisted: 88%**
Average Incident Remediation Time in Minutes	
Cohort 1 Baseline: 45 mins	**Cohort 2 AI-Assisted: 18 mins**

4. BROADER IMPACTS: DIVERSITY, EQUITY, AND WORKFORCE READINESS

Broadening Participation in Tech: Prioritizing deployment at community colleges and regional state universities where students often lack access to enterprise-grade security simulation gear.

Industry Alignment: Directly addressing the skills gap identified by the National Initiative for Cybersecurity Education (NICE) framework by instilling practical, portfolio-ready defense competencies.

Open Dissemination: Hosting annual regional workshops for faculty training and maintaining a public repository for all software modules.

5. PROJECT MANAGEMENT & GANTT TIMELINE

The 36-month grant execution is mapped across four structural phases:

[PROJECT TIMELINE & MILESTONES]

Year 1 (Months 1–12): Architecture & Alpha Testing
- Finalize containerized AI threat generation engine.
- Establish institutional review board (IRB) protocols for student data collection.
- Conduct alpha testing with 50 pilot students.

Year 2 (Months 13–24): Full Deployment & Quantitative Data Collection
- Roll out CyberSim-AI across 4 partner institutions (600+ students).
- Administer bi-semester technical assessments and behavioral logs.
- Mid-term independent program evaluation audit.

Year 3 (Months 25–36): Evaluation, Refinement & National Scale
- Aggregate multi-cohort dataset and perform psychometric/statistical analysis.
- Publish findings in high-impact STEM education journals (e.g., ACM Transactions on Computing Education).
- Public launch of the national open-source educator toolkit.

SECTION 6: EVALUATION & SUCCESS METRICS

The project will employ a rigorous data collection framework to measure both social and economic impact:

- **Economic Viability:** Percentage of incubator graduates generating positive net revenue within 6 months of program completion (Target: >80%).
- **Nutritional Output:** Total weight of fresh produce harvested, logged weekly through digital inventory sheets, and distributed to local food security networks and retail markets.
- **Participant Retention & Completion:** Graduation rates across training cohorts, measuring engagement, attendance, and business plan finalization (Target: >85% completion rate).
- **Environmental Impact:** Estimation of carbon miles reduced through local hyper-local food production and water conservation metrics achieved via efficient drip and aquaculture recirculation.