CIRCADENCE

# Building an Immersive Cyber Curriculum with Project Ares®

A use case from the
University of Colorado, Boulder

Circadence's Project Ares is an award-winning, immersive, gamified cybersecurity learning platform that helps students of all cyber competency levels apply learned concepts to real-world scenarios to build skills for the workforce. Project Ares delivers persistent, true-to-life experiences that match and adapt to current threats. The platform uniquely combines machine learning, single- and multi-player exercises, and offensive and defensive missions that mirror real-life scenarios.

## Project Ares Delivers

- AI-powered advisor adds in-mission support to help students through activities.
- Trainer View allows for real-time instructor engagement and additional depth in assessing, monitoring and reporting.
- Functional virtual machines simulate Windows, Linux, and Industrial Control System devices for comprehensive preparation on any system.
- Hyper-scalability with Microsoft Azure cloud enables cyber range learning capacity for classes, clubs, and competitive events of all sizes.

## Project Ares in the Classroom

Laura Lee, adjunct professor, taught a graduate level cybersecurity course using the platform at the University of Colorado, Boulder. To complement classroom taught concepts in the course titled, "Immersive Cybersecurity Defense," Laura holisitically incorporated the Project Ares platform into her course curriculum. Lectures coupled with the Project Ares lab environment allowed students to learn cyber theory and immediately apply it to real-world scenarios.

The following course syllabus is a sample to help fellow academic instructors visualize and conceptualize how a cyber range environment can be used to enhance student learning objectives within a cybersecurity course.

## Course: Immersive Cyber Defense

Students practice offensive skills in password cracking and exploit development to understand vulnerabilities and then focus on defensive tactics to reduce cyber risk and respond to cyber attacks. At the conclusion of the course, students will have experience using several real-world tools against actual threat attacks.

**The course is split into three units of study:**

**Unit 1:** Adversary tools and tactics

**Unit 2:** Cybersecurity work roles: Harden, Monitor, Pursue, Coordinate (Lead/Intelligence)

**Unit 3:** Defense teams tactics and procedures following the NIST Cybersecurity Framework

Students successfully completing this course should have an understanding of pathways to building expertise in the field of cybersecurity and the types of technical careers available.

## Learning Goals

Understand how an adversary develops a campaign to attack a network, including the types of motivations, tactics, and the kill chain pathway.
These concepts help defenders understand the data points that are present in an attack and where indicators of compromise can be found.

Understand the different types of work roles and technical competencies involved in cybersecurity defense.
Students will be exposed to multiple work roles and then choose the one that interests them for concentration during the course. Their selected work role will also be the basis of their specific midterm exam.

Apply cybersecurity defense knowledge across the full scope of the NIST Cybersecurity Framework to understand what defenders should do before, during and after a breach.

## Textbooks and Materials

**Required:** None
**Recommended:** Project Ares Media Center materials (or other sources on-line) on Linux System administration, Windows System Administration, Wireshark, Nmap, Snort/SecurityOnion, Metasploit
**Basic Tools:** Command line tools, Nmap, Wireshark, Snort (Security Onion), Metasploit

## Assignments

Weekly homework will be assigned as an activity in the Project Ares environment.

## Example Grading Mechanics

**Grading:** Midterm (20%) Final Exam (20%), Weekly homework (60%)
To do well in this course, students need to use the Project Ares environment to practice the concepts discussed in the classroom. Students are expected to explore the concepts and research the necessary topics and tools to be used. All homework will be assigned as an activity in the online lab environment. The exams will also be activities in Project Ares to be completed during the exam period.

## Sample Course Outline

| Week | Primary Topic | Objectives | Homework |
|---|---|---|---|
| 1 | Course Introduction | • Course overview<br>• Project Ares intro<br>• Cyber defender roles (NICE/NIST and careers in defense applicable to the course)<br>• CIA Triad and Adversary thinking<br>• Kill Chain Methodology | • Player Profile in Ares<br>• Battle Room (BR) 6 and 7 for Basic Linux and Windows<br>• Game - Cylitaire |
| 2 | Adversary Tools and Techniques | • Project Ares variability and scoring<br>• Intro to Kali/Metasploit tools<br>• Reconnaissance tactics (Nmap, Dig)<br>• Common Ports (ssh, telnet, vnc, http)<br>• Password Cracking techniques/tools<br>• M1 Easy walk through | • Game - PortFlow<br>• Mission 1 (M1) Easy + Medium (for extra credit) |
| 3 | Adversary Planning | • Using Nmap, hping3, Burp etc to understand network, fingerprinting, protocols<br>• Attack Surface/ATT&CK Framework<br>• Weaponization and Exploitation with Metasploit<br>• M2 Easy walk through | • Game - TacChain<br>• Mission 2 or Mission 3 (Easy or Medium) |
| 4 | Individual Work Role: Harden | • NIST/NICE and Work Roles for Teams<br>• Review Harden tasks and contrast with BR1<br>• Software Assurance and other common issues, OWASP<br>• Importance of Active Dir, OU/GPOs<br>• Firewalls | • Game - CyQual (Either Host, Net, Sys) Assessment<br>• Battle Room 1 (BR1) - system integrator |
| 5 | Individual Work Role: Monitor | • Review Monitor tasks and contrast with BR2<br>• IDS/IPS with Snort and Bro (Security Onion)<br>• Host and Network Monitoring<br>• Log Aggregation Techniques | • Game - RegExile<br>• Battle room 2 (BR2) - network analyst |
| 6 | Individual Work Role: Harden | • Review Pursue tasks and contrast with BR11<br>• Network Analysis with Wireshark<br>• System Integrity Checking<br>• Forensics | • Game - CyberVault<br>• Battle Room 11 (BR11) - host analyst |
| 7 | MID TERM | Work Role Assessment in class | Assessment Path, step 4 for either Network, Host or System Integrator |
| 8 | NIST CSF: Identify | • Critical assets and Key Terrain<br>• Mission Impact Model (MIM)<br>• Vulnerability Assessment (Nmap, Nessus)<br>• Understand Risk Management | Occam Analysis |

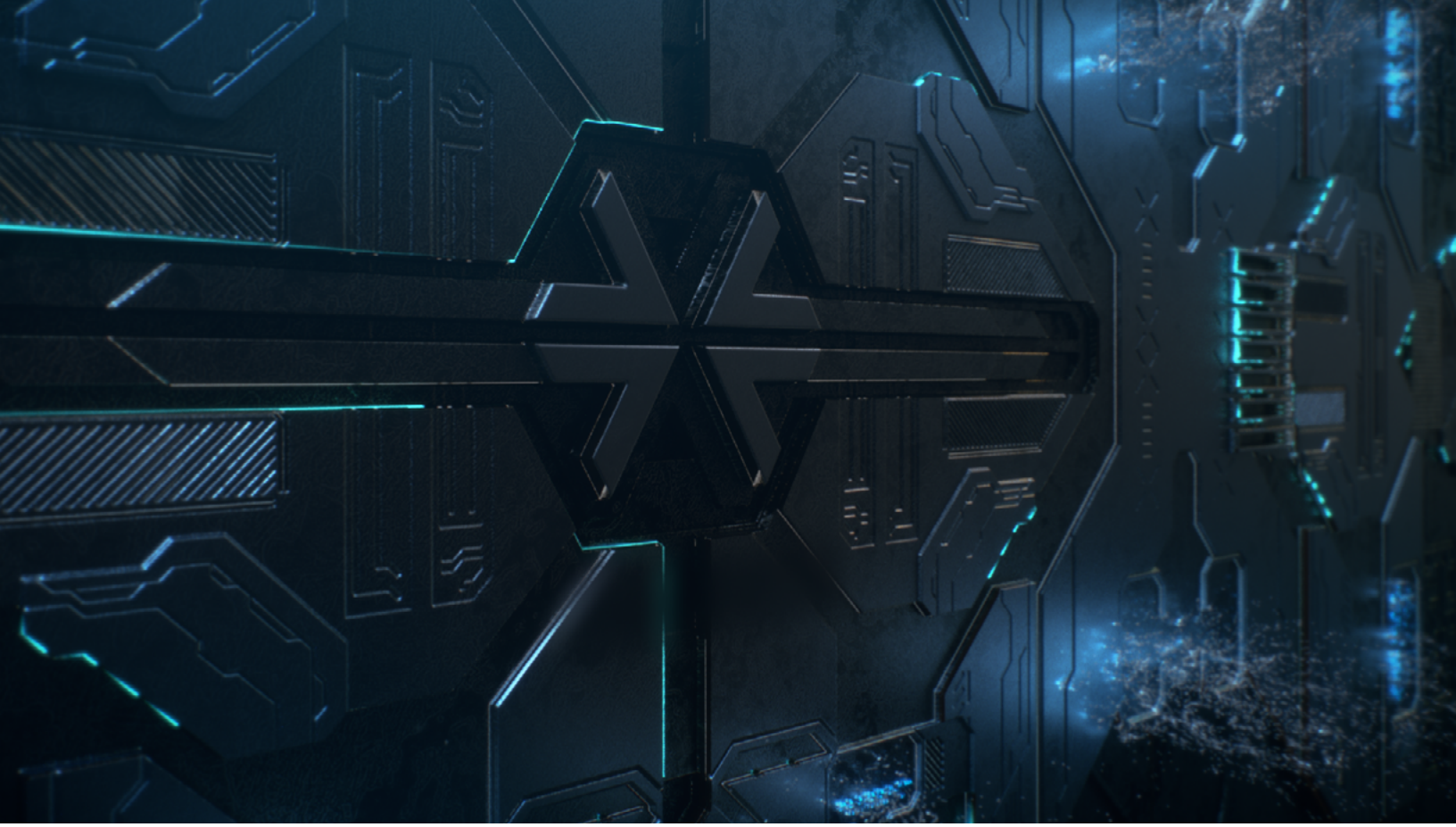
| | | | |
|---|---|---|---|
| 9 | NIST CSF: Protect | • Security Architecture<br>• Tailored Defense<br>• Lockdown Key Terrain (services)<br>• M5 walk through (malware analysis, alert, prevent malware) | Mission 5 (Easy or Medium) |
| 10 | NIST CSF: Detect | • IDS/IPS Rule Review<br>• Log Aggregation<br>• M4 walk through (packet capture, process analysis) | Mission 4 (Easy or Medium) |
| 11 | SPRING BREAK | | |
| 12 | NIST CSF: Respond | • Incident Response Process<br>• Workflow and hand off<br>• Role of Intel (and tension of rapid response) | Mission 10 (Easy or Medium) team play |
| 13 | NIST CSF: Recover | • Reporting<br>• Forensics<br>• BR9 walk through | Battle Room 9 (BR9) forensics |
| 14 | Team Tactics | • SOC Operations and Team Play<br>• A look at famous attacks (ransomware) and groups like Lazarus | Battle Room 10 (BR 10) Scripting |
| 15 | Review Course Q&A | • Trivia Loot Review<br>• Mission Walkthrough<br>• Prep for Final Exam | Mission 13 (M 13) individual or teams |



**Laura Lee,**

*Adjunct Professor at University of Colorado, Boulder*

Laura Lee brings an exceptional record of leadership in the field of cyber exercises and training, having previously directing the research and development at Johns Hopkins University/Applied Physics Lab. At Johns Hopkins, Ms. Lee developed the first ever Cyber Protection Team Crew Operations Manual for US Military Forces and National Guard Teams. In support of US CYBERCOMMAND, she led the assessment of cyber teams at large scale cyber exercises and developed team defense strategies.



## LOCATIONS

**Headquarters – Circadence Corporation**
1900 9th Street, Suite 300
Boulder, CO 80302

**Advanced Research & Development Facility**
398 E. Main Street, CDF Building, 2nd Floor
Tupelo, MS 38804

**Center For Cyber Autonomy & Data Sciences**
9665 Chesapeake Drive, Suite 401
San Diego, CA 92123

**Washington, D.C. Sales Office**
6715 Whittier Avenue, 3rd Floor
McLean, VA 22101

CIRCADENCE

Circadence® Corporation is a market leader in next generation cybersecurity readiness. Circadence's ecosystem is the first fully immersive, AI-powered cybersecurity learning and assessment platform for government and enterprise organizations.

Circadence's solutions modernize outdated and largely generic cybersecurity training with an advanced online gaming platform that delivers persistent, immersive and real-to life experiences that match and adapt to a contemporary threat environment. Contact us at 303.413.8800 or www.circadence.com/contact