CIRCADENCE

The Faces of Cyber Ranges

Tapping into Experiential Skill Building for Cybersecurity Teaching and Learning

Currently, the number of cybersecurity job openings across the United States exceeds more than 300,000[1] and experts predict 3.5 million unfilled positions will be a reality across the globe by 2021[2]. This, along with enterprise challenges to keep pace with imminent threats, hire and train, upskill and retain cybersecurity professionals, while affordably using the latest technology, is prompting academic institutions to teach cybersecurity skills in new ways to deliver the well-qualified cyber workforce organizations desperately need.

Used by military and commercial enterprises, cyber ranges have now captured the attention of academic institutions. In essence, cyber ranges provide emulations of actual networks, systems, and tools where novice and seasoned professionals alike can safely train in virtual environments[3]. They are used in the following ways:

As complimentary learning tools in the classroom

To train, test and assess cybersecurity professionals and students

To deliver and support cybersecurity events and competitions

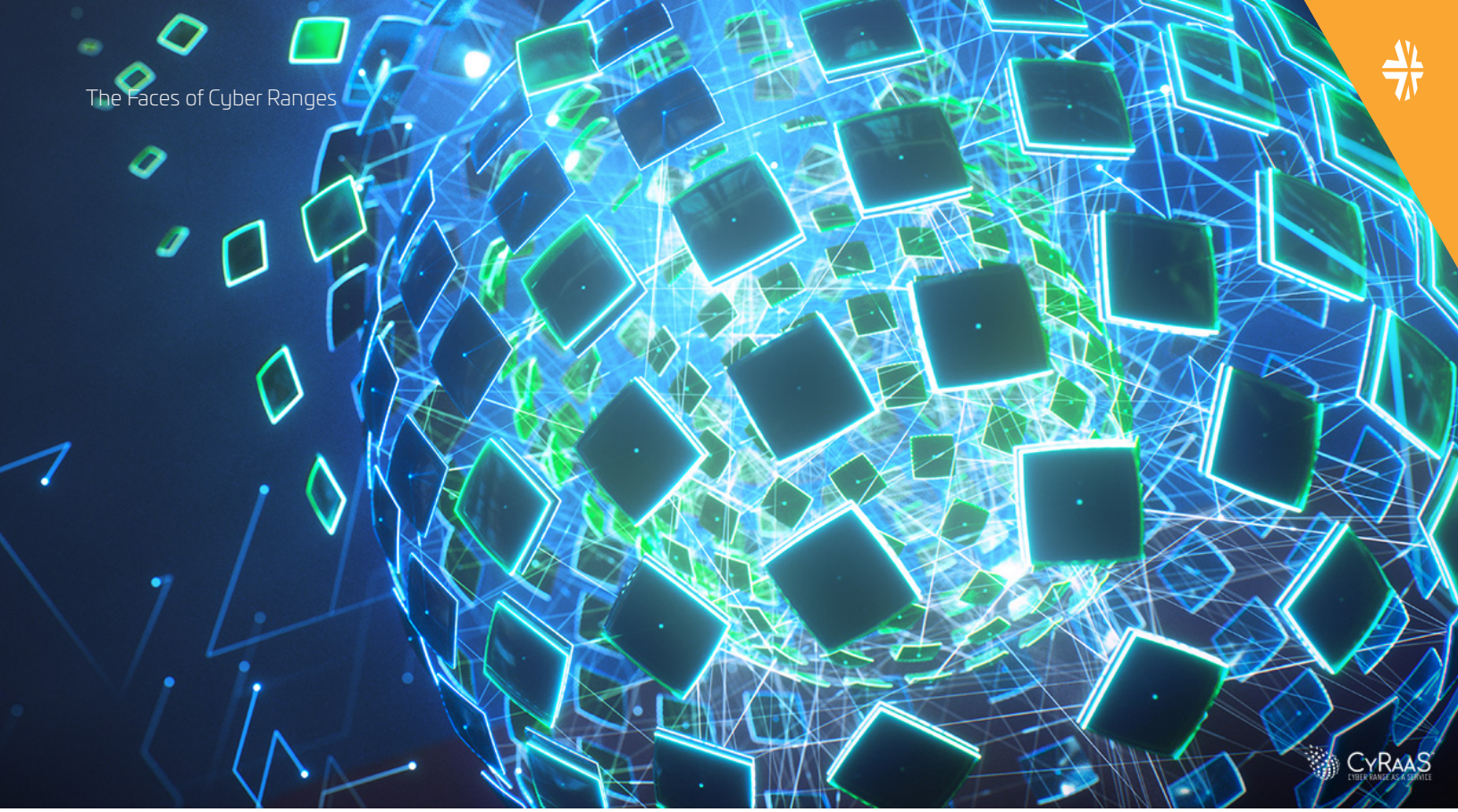
[1] CyberSeek, "Cybersecurity Supply and Demand Heat Map," National Initiative for Cybersecurity Education, Accessed 28 August 2018.

[2] Morgan, Steve, "Cybersecurity Ventures Jobs Report 2018-2021," Cybersecurity Ventures, 31 May 2017.

[3] NIST, "Cyber Ranges," National Initiative for Cybersecurity Education, Accessed 28 August 2018.

Training/Testing/Events–Project Ares®

Project Ares, the first gamified cyber range learning platform engages cyber students and professionals in mini-games, mission and battle room exercises to teach the basics, develop skills, reinforce cyber concepts, and expand one's knowledge base that will ultimately be put to the test in their professional lives. Its AI-powered in-game advisor, Athena, helps guide users through levels, adapting to individual learning styles for all skill levels. Project Ares has been used successfully for academic cybersecurity competitions, events and in the classroom to further student learning in fun environments at all levels of proficiency (K-12 through post-graduate programs). The platform's Trainer View allows instructors to monitor progress and see activity history of students in a report format.



Cloud and On-Prem Cyber Range Solution–CyRaaS™

Our premier Cyber Range-as-a-Service platform allows academic institutions the opportunity to train in realistic environments that mirror their actual company networks. The potential of CyRaaS is limitless, with the ability to support collective Nation State exercises as well as modeling for entire cities to develop living physical and fifth domain environments. Combined with Circadence's Project Ares, Orion Mission Builder™, and StrikeSet™, organizations can learn and grow without impacting your operations. This next-generation combination transforms traditional lecture-based learning, taking it out of the classroom and into interactive real-world environments, at any scale, anytime, anywhere.

The History of Cyber Ranges

Cyber ranges were initially developed by government agencies around the world that recognized how crucial highly-skilled cyber professionals would be to homeland security and national defense. In order to "make their state attractive to professionals seeking to move to locations with a more robust workforce[4]," they needed real-world, technical learning platforms. Initially, proprietary government programs involving defense contractors were the only programs that utilized cyber ranges. They served as the "proving grounds" for testing techniques, tools and procedures on classified networks[5].

> *One of the earliest examples of a cyber range is from 2002, called the U.S. Air Force SIMTEX (Simulator Training Exercise[6]). Early cyber ranges were developed for the U.S. Military in 2007 by Metova CyberCENTS and the Israeli Military in 2008 by Elbit[7].*

As technology advances, ranges are getting more sophisticated in their offerings , which will be discussed later in this paper. Today, such features help train the cyber workforce in government agencies and commercial enterprises. Now, universities, colleges and even high or middle schools are using cyber ranges to advance STEM learning at early ages and throughout the education process.

[4] Lohrmann, Dan, "Cyber range: Who, What, When, Where, How and Why?" GovTech.com, 10 March 2018.
[5] Lohrmann, Dan, "Cyber range: Who, What, When, Where, How and Why?" GovTech.com, 10 March 2018.
[6] Ritter, Ted, "Cyber Ranges: The Cyber Workforce Catalyst," LinkedIn, Accessed 28 August 2018.
[7] Ritter, Ted, "Cyber Ranges: The Cyber Workforce Catalyst," LinkedIn, Accessed 28 August 2018.

The National Initiative for Cybersecurity Education (NICE) recognizes the benefits of cyber ranges reporting they provide:

- Performance-based learning and assessment
- A simulated environment where teams can work together to improve teamwork and team capabilities
- Real-time feedback
- Simulate on-the-job experience
- An environment where new ideas can be tested and teams work to solve complex cyber problems

In order to effectively prepare the next generation of cybersecurity professionals, academic institutions are challenged to fuse the technologies of the field with the strategic thinking and problem-solving skills required to defeat today's hackers. Achieving this goal requires a fundamental shift in the classroom paradigm, adding alternative learning environments and strategies to the more traditional approaches. Furthermore, cyber ranges should be considered as a standing fixture in academic curriculum budgets. Just as medical schools partner with hospitals for programming that prepares students for positions in healthcare and as athletes train in state-of-the-art facilities to hone their abilities, so too can Middle/High/Primary Schools and Universities/Colleges have the technology and resources in place to train cyber professionals.

Academic institutions realize that in order to effectively prepare the next generation of cybersecurity professionals, they have to gracefully fuse the technicalities of the field with the strategic thinking and problem-solving skills required to defeat today's hackers.

What Are Cyber Ranges and Why Should Students Learn on One?

Cyber threats are ever-evolving and the quicker institutions can adopt cyber range training for student's skill development and learning, the better prepared students will be to address cyber threats in the real-world. Integrating the use of cyber ranges into curriculum can have direct effects on schools in several ways:

- Improve learning outcomes through experiential learning that is 'sticky'
- Enhance student enrollment and retention
- Build a school's reputation for STEM learning and cybersecurity leadership preparation
- Ensure student placement in business/government organizations seeking well-trained cyber professionals

By effectively preparing students for real-world attack scenarios in the workplace, academic institutions will increase their success rate of achieving learning outcomes pertinent to the cybersecurity profession. This can help lead to more funding to help with the critical continual improvement needed in curriculum and technology for a strong, ever-evolving cybersecurity program. On the student-side, hands-on cyber range education gives students the experience using actual tools found in the workforce, which in turn can help them find the best jobs.

Through our experience partnering with academic institutions, Circadence has observed first-hand how cyber ranges are being used in academic settings. We have identified the "faces" or identities by which such ranges manifest. Ranges are used for varying purposes including:

- Use in student learning and course development
- For cybersecurity department events and skill-building competitions
- For student training and assessment of skill level achieved
- For faculty training

Lessons Learned: Cyber Range Training Today

> *As institutions start to adopt cyber ranges to train cybersecurity students and improve learning outcomes, there are some challenges to be aware of among the more frequently used approaches.*

First, there are lessons to be learned from the traditional professional training methods used by government and enterprises today. Cyber professsionals often attend courses that are taught in the traditional lecture or PowerPoint-based classroom style at locations away from the office. The courses provide good concept-specific learning by going deep on narrowly defined topics, but are generally designed to teach offensive cybersecurity skills and are highly prescriptive when it comes to the process for submitting "answers" for scoring and assessment.

Circadence's observation is that these kinds of "presentation" driven approaches fail to coginitively engage professional cybersecurity learners and can negatively impact knowledge retention. When students routinely move through the motions, with little adaptation for different learning styles, the focus is on providing answers in the required syntax and not on absorbing the "how" and "why" nuances of an exercise.

> *As important as it is to learn about the "how" of cybersecurity attacks, it's understanding the "why" that can lead to effective defense.*

A more analytic, creative work flow style can help students learn both the fundamental skills as well as the critical thinking needed to adapt to new scenarios and threats. As important as it is to learn about the "how" of cybersecurity attacks, it's understanding the "why" that can lead to effective defense. Providing students the environment to learn and train within, fail within, and try again strong improves both the "how" and "why" skill progression.

As a result, some corporate cyber leaders are incorporating virtual cyber range learning into their professional development programs. Using ranges for experiential learning that evolves with the threatscape puts concepts into practice and keeps professional skills honed. Now, this perspective can also be applied to cybersecurity academic programs to help enhance current classroom teaching styles with real-world cyber defense application.

Not All Cyber Ranges Are Created Equal

Some traditional cyber ranges are fixed in specific locations and need to be built ahead of time, with pre-set, limited content. This can lead to a struggle to scale resources, trainers and adversaries.

Other cyber range solutions are dropped into current machine infrastructure without pause for content development or user experience. This hinders the true potential of a cyber range because it focuses on range use.

- Only from a hardware/infrastructure perspective for simple plug-and-play instruction
- Or only as a content delivery mechanism with limited infrastructure

In either circumstance, this minimizes the student's learning experience because they are not learning how to combat cyberattacks that reflect real-world networks.

What cyber learning options are available for academic institutions today? Let's review a few examples to better understand the strengths and opportunities.

Cybrary.it

Cybrary offers cybersecurity training videos to new and seasoned professionals alike. Users can create a free account to gain access to video tutorials but this does not include any kind of virtual lab environments. Videos are available by skill type or career level (e.g. beginner, intermediate, advanced). Users can select a career path to focus on, such as SOC Analyst or Ethical Hacker and have the freedom to choose what skill sets to hone.

However, the approach is passive in terms of information being absorbed by the student. And, while many small topics are broken down and addressed in detail, the overall strategic view of looking at complex, real problems is missing. The video access is individual and there is not opportunity to collaborate as a team, so learners do not work together in courses to defeat attacks as they would in a real-world exercise.

Practice Labs

Practice Labs provides virtual courses via video training and exercises, and offers integration to learning management systems (LMS) like BlackBoard. Data from the Practice Labs platforms can be funneled into gradebooks, enabling instructors' to more easily assess student comprehension and performance of concepts. Practice Labs' pre-configured real hardware environments are hosted in the cloud with accompanying lab guides for fast, convenient access to hands-on learning.[8]

[8] Practice Labs, "What is a Practice Lab?," Practice Labs Website, Accessed 28 August 2018.

The platform offers 24/7 access and students can engage with real equipment they would find in any work place. Student tracking and reporting capabilities and automated student fulfilment are added strengths to this cyber range option. However, the number of environments is limited, so student learning is restricted to the tools, content, and number of VMs available.

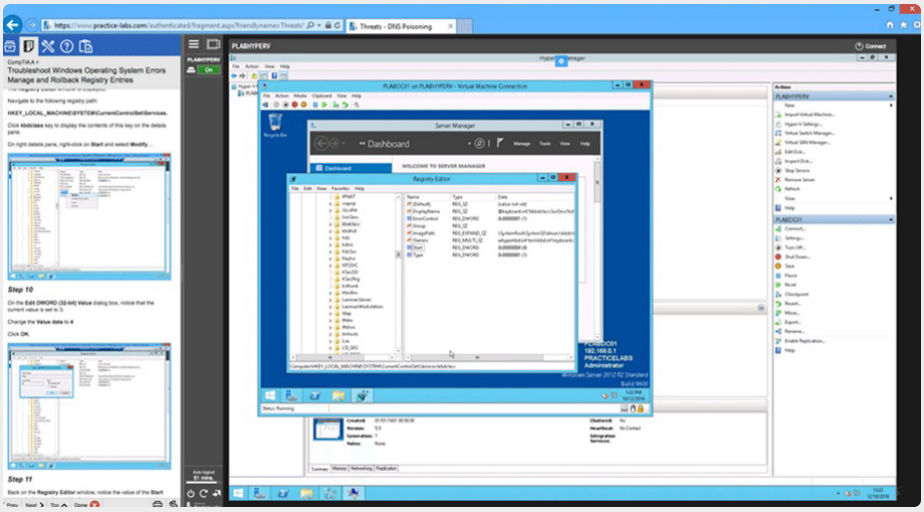


Figure 2: Screenshot of CompTia Practice Lab Course

National CyberWatch Center

National CyberWatch Center offers cloub-based labs developed by Infosec Learning for academic institutions to use immediately. The labs have step-by-step tutorials with technical envivronments to match, and the lab's Learning Tools Integration works with schools' LMS platforms allowing for single-sign-on capability. The shortfall of these labs is in their prescriptive nature and limited/siloed skill offerings (e.g. purchase access to a National CyberWatch Center lab on ethical hacking OR networking OR scripting) without the ability to train across disciplines.

Summing It Up: Critical Capabilities for Cyber Ranges

In the cyber range solutions discussed above, there are several key learning capabilities missing:

- Games for fundamental concept learning and skill-building with repetitive, hands-on learning style
- Defense strategy teaching, which requires multiple roles that can interact together in a problem-solving scenario
- Limited or non-existent scoring methods for detecting problem resolution status.
- Lack of team play for collaborative learning and greater strategic work.

These types of ranges also have at least one or more limitations.

1. Infrastructure-only ranges with no pre-programmed learning curriculum
2. Prescriptive, "check the box" approaches with fixed content
3. Limited number of virtual environments

Any or all of these limitations does a disservice to students who need current and accurate learning environments and materials that encourage trial and error necessary to be able to keep pace with evolving threats, new tools, updated operating systems. Further, a team-based training option is critical to learning the collaboration skills required in the real workplace. As Ted Ritter notes, "threats evolve much faster than conventional curriculum adapts[9]" and the same line of thinking can be applied to the types of limited range solutions mentioned above.

[9] Ritter, Ted, "Cyber Ranges: The Cyber Workforce Catalyst," LinkedIn, Accessed 28 August 2018.

Build Your Curriculum with Cyber Ranges

To ensure your academic institution gets the most out of its cyber range investment, the following features and capabilities should be considered to best maximize student learning and skill building.

1. Ensure the cyber range comes installed with pre-existing content that is informed by real-threat scenarios and attack methods.
2. Look for cyber range content that is diverse, offering a mix of both concept-driven exercises and real-world, team-based activities for well-rounded learning.
3. Consider custom mission builders (like Circadence's Orion Mission Builder) to create trainings that mirror the latest threats. This can help ensures the learning material is constantly evolving, just as threats are.
4. Assess instructor capabilities for reviewing and grading student performance to prevent tedium log review work.
5. Confirm that course syllabi and other learning materials can be integrated into the cyber range platform to tie learning objectives to actual student performance.
6. Consider Gamified activities that encourage students to "learn by doing," individually and in teams

These examples show that if not carefully evaluated, some cyber range solutions are actually more short-term skills training tools, rather than well-rounded, long-term learning and assessment solutions that leverage the full potential as outlined by NICE. In general, these simplisitic, virtual environments just do not cover the full spectrum of work roles and responsibilities required of today's cyber professional. Ultimately they are not the long-term effective tools needed to help address the widening gap of a highly-skilled workforce needed in government and commercial enterprise. Without realistic content and access to real world tools, students and instructors alike are left wondering if their academic training really prepared them in the best way possible.

The Next Generation Cyber Range

Circadence is redefining the modern cyber range with fully elastic, cloud-based solutions built from 25+ years of expertise, continued research and development, and 30+ patents across the fields of massively multiplayer online (MMO) gaming, latency and optimization. Deployment scenarios are "cloud agnostic", delivered via:

- private, Infrastructure-as-a-Service partners
- public cloud providers – like Microsoft's Azure intelligent cloud

Through any of these providers, the Project Ares learning platform from Circadence is accessible to students, anywhere, anytime, 24/7 with an active internet connection and a modern web browser.

> *This learning environment includes threat scenarios across a variety of industries, enable users to spin up 3-50+ VM environments to support mission play, and is a safe space that encourages exploration, trial and error, and hands-on practice with cybersecurity skills, tools, and scenarios.*

Built in the cloud and served through web browsers, the gamified, AI-powered platform can be accessed by students independently or in teams, without compromising the institution's actual network. This learning environment includes threat scenarios across a variety of industries, enable users to spin up 3-50+ VM environments to support mission play, and is a safe space that encourages exploration, trial and error, and hands-on practice with cybersecurity skills, tools, and scenarios. The unprecedented flexibility allows for, and encourages, exponential growth in both scope and scale.

Project Ares: The "Face" of a Next-Generation Cyber Range

Via Project Ares, Circadences delivers a level of gamification that positively changes the landscape for cybersecurity education, learning and assessment. Not only does this work to connect the dots in making cyber ranges accessible to users at all levels of proficiency, it appeals to/makes cybersecurity applicable to individuals without IT/cyber in their background or title.

> While our "face" looks very much like a game, and our roots in massively multiplayer online (MMO) gaming run deep, it's important to recognize the difference between games and gamification.

Digital games are not real; gamification can be. In the case of Project Ares, it is very real. When done well, gamification takes advantage of brain science to use the concepts of gaming (i.e. levels of difficulty, chat boxes, points and scoring, leaderboards, digital badges, etc.) within a learning environment.

In fact, this type of active learning, where hands-on experiences drive cognitive retention, serves learners by meeting them where they are in the learning process. Studies show active-learning models increase information retention to 75 percent compared to 5 percent with traditional, lecture-based education[10]. High engagement in cybersecurity education is critical because if students are not interested in learning new skills, and aren't encouraged to think outside of the box, they won't be adequately prepared to handle threats that are always changing and evolving in the workplace.

The cyber range "face" that is Project Ares, combined with our efforts to leverage artificial intelligence in learning, means as students grow, the cyber range scales, too. Circadence's patented application of artificial intelligence means students will always have an instructor at their fingertips so students receive immediate feedback, and ensures content is delivered to meet their learning needs.

The Content

Project Ares delivers learning, training, and assessment opportunities to anyone from cyber newbies to cyber ninjas, with both individual and team-based engagements. It can be adapted to students in undergraduate and graduate university programs as well as Middle/High/Primary level schools.

Media Center

The Media Center built into Project Ares serves students with a plethora of case studies, white papers, news articles and video tutorials across a vast range of cybersecurity topics. These resources are educational in nature, cover everything from introductory/fundamental concepts to the highly technical. The Media Center can be modified by academic institutions to deliver the necessary digital media files in support of each unique class or program.

[10] Play to Teach, "Solving the training dilemma with game-based learning," Digitech, Accessed 28 August 2018.

Mini-Games

Figure 3: Mini-Game Library

Built in Unity3D, the Mini Games available within Project Ares are designed to introduce students to and encourage consistent engagement and repetition of core cyber skills, technical, and/or operational concepts. The Mini Games are modeled after traditional games that should feel familiar to most students, such as Solitaire, Jeopardy, memory/ matching games, etc.

Each game provides a tutorial to introduce the skill and teach a student how to play, and also includes hints to enable player success throughout the game. Multiple levels of gameplay increase in difficulty and require students to demonstrate growth in proficiency. The goal of these mini-games is to provide a fun and instructional way to learn a new concept or stay current on perishable skills.

Battle Rooms

Figure 4: Battle Room Selection

Various Battle Room environments built for Project Ares allow individual students to go more in-depth by practicing focused hands-on tasks that tap into the cyber range and interact with virtual machines defined in a unique network map. These Battle Room exercises are mapped to the NICE Cybersecurity Workforce Framework and can be easily aligned to course syllabi.

Each Battle Room environment is built to reflect a specific learning track or work role (i.e. Linux Basics, Digital Forensics, Network Technician, etc.), and students can launch a Virtual Network Computing (VNC) or Secure Shell (SSH) terminal to execute command line exercises, navigate a more traditional desktop interface, or engage with a series of built-in tools. Project Ares can even allow students to introduce resources and tools into the environment via their SSH terminal, configuring them on the fly and adding to the simulated world inside the Battle Room.

The Project Ares AI-powered, automatic umpire supports Battle Room engagement by providing students with in-real-time feedback, as their completion of tasks leads to points earned and fulfilling visual confirmation. Further, all student data–down to individual key strokes, hints used, chat messages shared, completion of tasks, lessons learned, etc., – are saved and recorded to student profiles as both Excel files or DVR-style videos for submission or future review.

Mission Scenarios

Figure 5: Mission View High Scores

Offering curriculum that is both offensive or defensive in nature, students will be presented with real-world situations (i.e. networks that reflect the financial industry, healthcare, energy grids, water treatment facilities, and other critical infrastructure) and charged with piecing the knowledge together in a display of conceptual understanding and technical proficiency.

Mission scenarios are available in the professional license option through Circadence and are designed to teach real-time, collaborative end-to-end problem solving.

Unlike Battle Room environments, Mission objectives will build on each other, evolve throughout the Mission play, and require student's to disable botnets, remove malware, defend power grids or against web attacks, etc. Complex and highly customized network maps serve as the "learning space" for Mission scenarios, and the multiple levels of difficulty offered for each Mission allows for additional variability and unique challenges that match each student's skill maturity. Team play can also be mandated to encourage students to delegate tasks and reinforce collaboration, and the actions of the AI-powered background network adversary is designed to keep content fresh and students on their toes.

Assessment Pathways

The Assessment hot spot in Project Ares allows students to train on scaffolded activities that mirror certification requirements or any other set of pre-defined content or curriculum. These activities are installed as modules, with students unlocking each module progressively as they meet a certain level of proficiency on the previous engagement.

Trainer View

In addition to the student benefits of adopting Project Ares to support academic efforts, faculty and departments also benefit from its Trainer View feature, which offers additional depth in monitoring, assessment, performance data and skills reporting. Cyber instructors are able to:

- Adjust settings within the environment (e.g. turn off and on hints, the in-game advisor, and the background network adversary)
- Publish Live Leaderboards
- Extract data and reports at both the individual level and across cohorts for a designated time period
- Add comments to a student's log file while they're in session
- Modify the live environment for students in real-time

Figure 6: Mission Trainer View

To accomplish these last two capabilties, the Trainer View available within Project Ares enables the Trainer to shadow users by bringing up the students' terminal while it's active. Once in a student's terminal, the Trainer can act as the background network adversary anonymously and pivot or enumerate in the network, adjusting the environment on the fly based on the user's progress, skills or struggles.

Students who train on next generation cyber ranges like Project Ares will ultimately be able to improve the security posture of the organization's they work for because they will be able to respond quicker, detect threats and vulnerabilities faster, think like hackers, and inspire fellow colleagues to take cybersecurity training seriously.

Students who train on next generation cyber ranges like Project Ares will ultimately be able to improve the security posture of the organization's they work for because they will be able to respond quicker, detect threats and vulnerabilities faster, think like hackers, and inspire fellow colleagues to take cybersecurity training seriously.

Persistent Cyber Range Learning will Help Students Be Better Prepared to Enter the Cyber Workforce

Today's students require a modern approach to cyber education—one that adapts to their online learning styles, engages them with unique game-play storylines, and shifts the overarching paradigm from static and skill-based to dynamic and AI-powered learning.

Cyber range solutions have come a long way from the military-based usage of 2002, but much more work can be done to ensure the next generation of cyber professionals are prepared to defeat evolving threats. Academic institutions have an exciting opportunity in front of them – to lead the way with progressive, next-generation learning approaches that use cyber ranges to better prepare students for the dynamic workplace. Instituions and instructors can maximize their cyber range investments by thorough review of range capabilities. A high-fidelity, cloud-secure range can help empower today's cyber training and learning challenges.

Watch a video and learn more about Project Ares and other cyber learning solutions at https://circadence.com.

303.413.8800 • www.circadence.com • sales-cyber@circadence.com

HEADQUARTERS Boulder, CO 80302
ADVANCED RESEARCH & DEVELOPMENT FACILITY Tupelo, MS 38804
CENTER FOR CYBER AUTONOMY San Diego, CA 92123
WASHINGTON D.C. SALES McLean, VA 22101