CIRCADENCE

Upskill Cyber Teams with Artificial Intelligence and Gamified Learning

How to Automate, Augment, and Better Prepare Cyber Professionals

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD

SC 2019 awards Winner

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

Executive Summary

CISOs are aware that the cybersecurity skills gap is impacting organizational security readiness both on a professional level and at a company-wide level. Typically, team collaboration improvement programs, performance assessments, and periodic professional development activities are enough to cultivate a stronger workforce—but when it comes to the cybersecurity industry, we are in another ball game. The nature of the expanding and escalating threat landscape means that continual upskilling of the cyber team is a business imperative. Today's hardworking cyber workforce is strained, stressed, and depleted, leaving many executives to ask: what options do I have? That's where artificial intelligence and gamified cyber learning come into play. In the wake of imminent threats, these new approaches encourage progressive skill building partnered with friendly team competition to improve security readiness efforts through hands-on, learn-by-doing activities. We propose organizations looking to upskill cyber teams and improve cyber preparedness can do so using AI and gamified learning.

A New Cyber Approach is Needed

You don't have to look far to realize that the cybersecurity industry is in desperate need of new approaches to help adapt to the speed of threats. News headlines remind CISOs and business leaders of the impact of breaches, from financial to reputational damage and loss of trust. When it comes to the importance of strengthening organizational security posture, oftentimes, it starts with who is on the digital frontlines defending corporate assets.

The growing lack of cyber talent, low retention, and tight budgets stack the cards against cybersecurity professionals and industry leaders who work hard to build the strategies that will prevent attacks on their organization. *A report from (ISC)*[1] found that the global cybersecurity workforce will have more than 1.8 million unfilled positions by 2020[2]. This leaves current cyber professionals spread thin. One can imagine the severity of such a deficit when cyberattacks keep slipping through the business cracks:

- According to *Harvard Business Review*, "the average company handles a bombardment of 200,000 security events per day[3]."
- About 54 percent of companies[4] experienced one or more successful attacks that compromised data and/or IT infrastructure.
- It's estimated that more than 80 billion malicious scams are conducted every day; 300,000 new malware strains implemented; 33,000 phishing scams conducted; 4,000 ransomware activities; and 780,000 records lost to hacking[5]—leaving lots of businesses struggling to keep up.

[1](ISC)², "Global Information Security Workforce Study," 15 February 2017
[2]Gartner, "Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017," Gartner Newsroom, 7 December 2017
[3]Kolochenko, Ilia, "How artificial intelligence fits into cybersecurity," CSO, 31 July 2018
[4]Ponemon Institute, "The 2018 State of Endpoint Security Risk," Ponemon Institute, October 2018
[5]McAfee, "Economic Impact of Cybercrime – No Slowing Down," Accessed 11 March 2019

The result is cyber teams who are exhausted from long hours, lots of pressure, and unreasonable workloads, which leads to dissatisfied employees and high attrition rates. This is a serious problem because organizations that are trusting their data security to a weary cyber team are ultimately a threat to all of us.

Artificial Intelligence Automates and Augments the Cyber Workforce

A new way to address security readiness lies within the power of artificial intelligence. It can be used for more than programming robots and self-driving cars. Many companies are finding that a hybrid approach is the most successful, where everything that can be automated with AI is, and the rest relies on human intelligence[6]. AI and machine learning emulate human cognition (e.g. learning based on experiences and patterns rather than inference) and use deep learning advancements to 'teach themselves' how to build models for pattern recognition.

This becomes particularly valuable in cyber skills development where Natural Language Processing (NLP), a sub-field of AI, can communicate with human during cyber exercises and aid progression through activities. NLP is present in our cybersecurity learning platform *Project Ares®*. The in-game advisor, Athena, uses NLP to communicate with players in a "chat-bot" format bringing the student answers to questions, providing guidance to help complete tasks and meet learning objectives. Athena generates a response from its learning corpus, using machine learning to aggregate and correlate all the player conversations it has plus integrating knowledge about how users progress through exercises. The pattern recognition helps Athena recommend the most efficient path to solving a problem or scenario. Similar to the "two heads are better than one" motto, but machine learning needs lots of "heads" (aka: data) to generate the best solution for the problem at hand.

Likewise, AI is used to create the adversary in Project Ares mission exercises. It is used as a force multiplier for offensive capabilities. Specifically, machine learning models provide a general mechanism for organization-tailored obscuring of malicious intent, enabling adversaries to disguise their network traffic or even on-system behavior to look more typical to evade detection. In addition to enhancing data exfiltration capabilities, these techniques provide the capability to continually model and adapt even after deployment, enabling them to persist undetected for longer. These techniques challenge the offensive player in a good way, so they begin to think like the unauthorized user and understand their response to defensive behavior. This added capability provides greater learning potential for users who are not only using defensive techniques with AI but also using offensive techniques with data AI provides.

Companies like Uber have already jumped aboard the AI train. They use machine learning to understand the various routes drivers are taking to transport people from point A to point B and it then uses all that data to predict the most efficient routes. The result: current and future Uber drivers can better serve their passengers. Mission accomplished.

Now imagine that same concept applied to cybersecurity professional training. Cyber professionals engage in a learning platform that offers relevant cyber exercises to build skill and competency with the support of artificial intelligence, NLP and machine learning on-hand.

[6]*Kolochenko, Ilia, "How artificial intelligence fits into cybersecurity," CSO, 31 July 2018*

Professionals learn better ways to offensively and defensively protect their companies, build new skills, and develop problem solving tactics in real-world scenarios all at the same time. **That is a powerful approach to professional development that is more utilitarian and meaningful than a periodic, off-site cyber training course rooted in passive learning models like PowerPoint presentations.**

> Today we see AI used to help classify good vs. bad email for improved detection of phishing campaigns. It is also used to analyze user behavior (as normal or anomalous) for both fraud detection and malicious network activity. Other emerging uses of AI for cyber include automated log aggregation and enrichment data from multiple sources, virtual assistants with special knowledge in cyber, augmentation of operators for penetration testing and automated instructors, opponents and scoring for cybersecurity training.
> *~ Laura Lee, Executive Vice President of Rapid Prototyping, Circadence*

Forbes contributors identify the potential of such a deployment, noting:

> "…when you combine very smart security personnel with adaptive technology that continues to change and become smarter over time, you provide a competitive edge to defenders that has primarily been absent from most cybersecurity technologies to date.[7]"

That's why it's vital to re-skill and develop your cyber team so they can successfully prepare for anything that comes their way.

The more cybersecurity professionals engage with the Project Ares platform, its AI capabilities and its curriculum, the better information data scientists have to draw on when building new ways to solve today's cyber scenarios. **The more efficiently professionals solve cyberattack scenarios, the quicker they are to defeating incoming threats, and the more they contribute to protecting companies and closing the skills gap.**

Another exciting outcome of AI is in its ability to assess the cyber workforce. AI can be used to score or rank activity performance. This is a valuable function to help CISOs understand where the skills gaps are within their teams, enabling them to put evaluation programs in place to build stronger, cross-functional teams with the right mix of skills to analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend and securely provision. Further, data from the assessment scores can be used to identify new cyber exercises that can be created to keep learning content fresh—saving time and resources for cyber learning managers who are trying to figure out what pathways to develop to best support teams.

[6]*Forbes, "How Will Artificial Intelligence and Machine Learning Impact Cyber Security?," 15 February 2018*

> …the only cost-efficient and scalable mechanisms for detection and remediation are quickly becoming artificially intelligent systems with the ability to sift through largely unstructured data, identify malicious behavior over potentially long time horizons, and dynamically respond.
> *~ Bradley Hayes, Chief Technology Officer, Circadence*

The relationship between AI and cybersecurity comes down to how it is used within a solution and the quantity and quality of data it has available to work with. In the case of Project Ares, AI helps guide and teach trainees during game play, giving them new threat vectors, scenarios and tasks based on past performance and behavior. In other words, the ecosystem feeds threat data to improve training, augmenting cyber actions to ensure players are learning best practices to combat evolving threats.

What we've learned from the power of AI is that with a large corpus of data to work from, it is the most productive way to ensure systems take the best actions for the player's learning advantage—and players, too, make informed decisions that help them defeat emerging threats.

Gamified Learning Enables the Cyber Workforce

As the cybersecurity field has developed from a function within IT into a mission-critical business function, cyber training has continued to be delivered primarily in classrooms or on-demand videos with an instructor lecturing to passive listeners. While this learning model has been around for a long-time, it is not effective for cybersecurity where threats are ever evolving, business risk is ever escalating, and learning to adapt to new threats must be ever on-going. **Curriculum needs to evolve as rapidly as threats do;** it is not sustainable or reasonable to ask learners to figure out how to adapt and defeat attacks that were simply "not known" when they went to class three, six, even 12 months ago. Further, the passive learning model is known for inviting cognitive disengagement. *Studies*[8] show people forget:

- 40% of what they've learned after 20 minutes
- Between 50-80% of what they've learned after one day
- 77% of what they've learned after six days
- 90% of what they've learned after one month

Not only is the material forgotten, but if there is only minimal opportunity to have hands-on experiences with learned concepts, then students don't learn to analyze and think critically about the material in a meaningful way.

There is a better way to enable cyber teams and it is through gamified, active learning. Gamification is a logical step in training the *next gen learner* (born after 1980), who has never known a world without video games. Gamification is often defined as the process of adding games or game-like elements to something. The term was originally coined in 2002 by a British computer programmer named Nick Pelling. Gamified learning is a natural progression for cyber skills development that incorporates a style of teaching best suited for today's professional.

[8] *Tartell, Ross, Ph.D., "Strategies to Make Learning Stick," Training magazine, Accessed 14 February 2019.*

> We've found that by gamifying cyber training, making it fun and engaging for learners, that they have better retention rates.
> *~ Keenan Skelly, VP of Global Partnerships and Security Evangelist, Circadence*

Unlike compliance-driven teaching methods, gamified teaching engages practitioners individually and in teams, through modern learning strategies. It works by **enabling learners to apply what they know to simulated environments or "worlds," creating a natural flow that keeps learners engaged and focused.** Further, it can deploy connected, interactive, social settings that allow learners to excel in competitive, strategic situations. Organizations that offer gamified exercises to teams report that *96% of workers see benefits*[9] including increased awareness of weaknesses, knowledge of how breaches occur, improved teamwork and response times, and enhanced self-efficacy.

In gamified environments, trainees are typically:

- **Rewarded** for good behavior
- **Incentivized** to maintain good behavior
- **Encouraged** to dialogue about their lessons learned with peers
- **Reminded** of what they don't yet know and held accountable
- **Engaged** in their progress thanks to leaderboards
- **Prepared** to combat any threat scenario

To teach and hone skills, Project Ares offers mini-games to learn concepts, battle rooms to practice tactics, and missions to learn by doing on cyber ranges. The virtualized environments allow players to learn about both offensive and defensive tasks and protocols. Full-scale missions portray real-world cyberattack scenarios, like the WannaCry ransomware that disrupted medical devices, and offensive exercises covering adversary tactics are also available. Players use real-world commercial and open-source tools incorporated into mission design or they can add in new ones or write their own to see what works best with evolving threats.

As players engage in these activities, they earn experience points that lead to skill badges to bring forth the "gamified" aspect of learning—all of which is viewable on the platform's leaderboard. They are also able to play individually on the platform or in teams. **In a naturally competitive way, players can have that hands-on experience they've been craving—even the experience of failure, which is critical to learning and growing.** There are work role learning paths aligned to the NIST/NICE framework to standardize learning and the platform can help professionals take what they've learned in their certification work and apply it to realistic scenarios.

Gamification, as a new paradigm for learning and exploring, is used today with the military and enterprises. It is also being used effectively in K-12 schools and universities nationwide. Whether building security awareness in middle and high school students or complementing higher education classes as a real-world lab, Project Ares is helping to build the next generation of cyber professionals.

[9]*Ashford, Warwick, "Automation and Gamification Key to Cyber Security," ComputerWeekly.com, 3 April 2018.*

Continuous Learning to Empower Cyber Teams

While certifications and technical degrees are a starting place for cybersecurity readiness and workforce development, CISOs must think about new methods that provide the persistent access to cyber education to keep staff actively engaged in critical learning. As we know in this industry, the only constant in cybersecurity is change, and for that reason (in addition to the multitude of attacks every day), **we must be vigilant in putting learning to work for us.**

The ability to continually develop skills and knowledge necessary to perform effectively in a changing environment is a necessity today. Cyber professionals must be willing to stay current with the latest threat tactics and continually apply new knowledge to protect their enterprise or agency data as well as sustain/advance their own careers. With on-going understanding of how malicious hackers operate, what tools and tactics they are using, how offensive techniques can improve, and how human and machine can work together in sync to reduce risk, the better off everyone will be.

Today, CISOs can collaborate with their teams in building professional development plans with the following in mind:

1. Interview and assess cyber teams to identify skills deficits and, therefore, understand what team members need to learn/develop.
2. Address large workloads via automation and augmentation so that cyber teams can move away from data handling tasks and into higher-level reasoning and analysis.
3. Provide ample opportunities for skills development through gamified learning, mentoring, networking, and continuing education.
4. Develop teams incrementally and continuously via a "day-by-day, month-by-month" mindset – as the job is never done in this field.
5. Dedicate resources, set expectations, and align corporate culture with the goal of enabling employees to get the learning they need to protect and defend the organization at every stage of their careers.

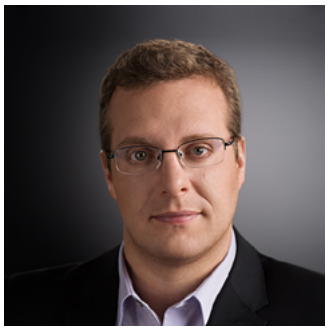
Increased understanding, skill and application of offensive and defensive strategies using gamified learning supported by AI, will greatly improve an organization's security. As technology and interconnectivity evolve with each passing day, steps must be taken immediately to adopt a culture that values and emphasizes continuous learning to avoid an organizational attack headlines in tomorrow's newspaper. With AI and gamification at the helm of a new learning approach for cybersecurity, we can be on our way to minimizing the cyber skills gap, empowering existing cyber teams, confidently hiring new cyber staff, and harden organizational security posture in a more effective way.

For a full in-depth overview and demonstration of how Circadence's next generation learning and assessment solutions can empower and enable human cybersecurity teams, reach out at *www.circadence.com* or call 303.413.8800.

Contributors:

Laura Lee,
Executive Vice President of Rapid Prototyping

Laura Lee leads development around the company's AI-powered, multi-player cyber learning platform, Project Ares. 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, prior to joining Circadence. 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.

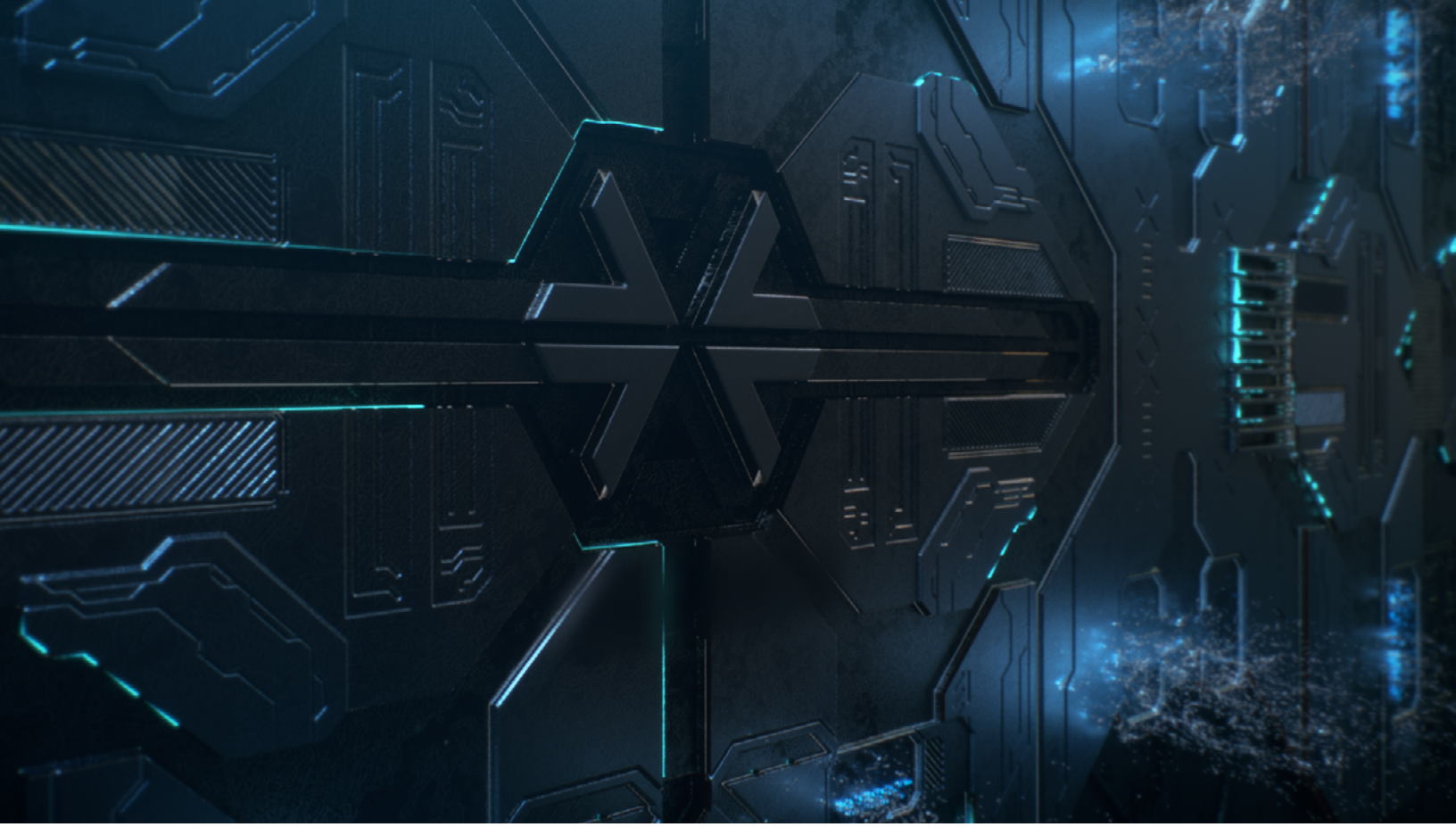


Bradley Hayes,
Chief Technology Officer

With decades of professional experience, Dr. Hayes' expertise in Artificial Intelligence and Machine Learning supports continual innovation for Circadence's cyber readiness solutions. Hayes teaches as a professor at the University of Colorado's Department of Computer Science and serves as the Director of the Collaborative AI and Robotics (CAIRO) Lab. He has in-depth experience developing techniques to build autonomous AI that can learn from and collaborate with humans, making people more efficient and capable during task execution.

Keenan Skelly,
Vice President of Global Partnerships & Security Evangelist

As a former U.S. Army Explosive Ordnance Disposal Technician and former Chief for Comprehensive Reviews through the Department of Homeland Security, Skelly's extensive experience in government service informs her current responsibilities as an executive woman in cybersecurity. She has 20 years of experience providing security and management solutions across a wide array of platforms to include personnel, physical, and cybersecurity. Her expertise in crisis management, intelligence analysis, law enforcement and emergency management make her an admired and respected leader among her colleagues.



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