Whitepaper

Cyber Range Simulations

Advancing Cybersecurity Skillsets in Realistic Virtual Environments

OffSec
The Path to a Secure Future™

The average breach lifecycle is 287 days, with organizations taking 212 days to initially detect a breach and 75 days to contain it.[1] Why the enormous delay? The state of cybersecurity is extraordinarily tenuous. Cyber attacks are on the rise, attackers are increasingly agile and creative, breaches are growing more sophisticated, and many cybersecurity teams lack the skills needed to identify and mitigate new and evolving threats.

The world of cyber crime is a dynamic one, powered by a flood of new players and strategies focused on unleashing a steady stream of cyber attacks. While cyber experts may receive intense theoretical, in-person and online training, experiential training is what they need to effectively combat their adversaries. Cyber ranges provide just that, giving cyber security professionals a simulated lab where they can train, test, and practice their response to cyber attacks in a realistic, yet safe environment.

This whitepaper will dive into the purpose and importance of cyber ranges, potential use cases for today's modern businesses, and finally the benefits to the individual professional, the cybersecurity team, and the organization as a whole.

1 Experiential training for cyber defense

Cyber attackers not only exploit vulnerabilities to steal an organization's personal and proprietary data, but they can also pose significant danger by interrupting or destroying essential services. To combat these increasingly sophisticated threat actors, organizations should prepare for cyber attacks the same way the military prepares for attacks on the battlefront–with experiential training.

No matter how skilled cybersecurity experts may be, they can only learn so much from instructors, classes, books, and videos. To win the battle they need hands-on training using realistic training environments that prepare personnel for real-world cyber warfare and cyber defense. Cyber range simulations are akin to flight simulators for today's fighter pilots, which give them the ability to learn, fail, and succeed in a safe environment that mimics a real-world experience–without the risk of real-world consequences.

In fact, the military and government were the first to develop and use cyber ranges to simulate cyber threats and test the effectiveness of defensive strategies. As cyber threats intensified, tech companies and cybersecurity providers realized that existing theoretical learning and static scenarios failed to fully prepare teams for the dynamic nature of cyber threats. In response, they developed commercialized cyber range solutions that provide a safe and controlled space for hands-on cybersecurity training, testing, and experimentation.

2 Why cyber range simulations are so important

1. Cyber threats are rising.

The pace, volume and reach of cyber attacks continue to intensify, affecting enterprises and small and medium-sized businesses across almost every industry. Consider these statistics:

38% Cyber attack	Cyber attacks increased by 38% globally in 2022 vs. 2021 and are only expected to grow in sophistication, frequency, and volume.[2]
450,000 New malware	450,000 new malware are created daily.[3]
41% Ransomware breaches	Ransomware breaches grew 41% in 2022 and took 49 days longer than the average breach to identify and contain.[4]
80% A third-party-related breach	And an astounding 80% of organizations have suffered a third-party-related breach in the past year.[5]

More than ever, today's organizations must be prepared for the constantly changing cyber battlefield where increasingly sophisticated cyber attackers are launching new threats all the time.

2. Organizations are paying a huge price.

Year over year, organizations are facing increasingly severe consequences resulting from cyber attacks–including a damaged reputation, customer attrition, and revenue loss. 83% of consumers will stop spending with a business for several months in the immediate aftermath of a security breach, and over a fifth (21%) of consumers claim they will never return to a business post-breach.[6] Additionally, businesses are facing massive regulatory fines. The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years,[7] and globally, damage from cyber attacks is expected to increase by 300% over 10 years.[8]

3. Recruiting cybersecurity talent is a challenge.

Hiring cybersecurity talent has become a daunting challenge. A staggering 60% of organizations are struggling to recruit qualified cybersecurity professionals, while 67% believe that the shortage creates significant risks to their company.[9] This talent shortage could quickly become a cybersecurity crisis, with Gartner predicting a lack of talent will be responsible for over half of all significant cyber incidents by 2025.[10]

4. Cybersecurity teams aren't prepared due to a skills gap.

Even though over 93% of cybersecurity experts and 86% of business leaders believe a catastrophic cyber event is likely in the next two years, 34% say they lack the skills needed within their cybersecurity teams to prevent one.[11] There is a cyber expert shortage and talent gap that looks like it will be widening due to stress, work overload, skill shortage, burnout, and low morale. 64% of cyber security leaders have seen a rise in staff turnover, with 20% of cyber security professionals considering leaving their current role in the next six months.[12]

5. Taking a proactive approach to ongoing cybersecurity is critical.

When an organization is attacked, cyber experts don't have time to slow down and think. Instead, they need the skills and confidence to react within that pressure cooker environment. Organizations can create a stronger, ongoing proactive approach to cybersecurity by arming cybersecurity experts with the knowledge and training they need to feel prepared and confident during a real-world attack. To accomplish this, cybersecurity experts require continuous, hands-on training that simulates the circumstances and pressure of a real threat.

Cyber ranges play a crucial role, offering a safe, controlled, and realistic environment for organizations to proactively train their teams, test their defenses, and improve their response to cyber threats. They allow teams to practice dealing with real-world scenarios, make mistakes, and learn from them in a risk-free environment. And cyber ranges can accommodate different learning styles, enabling personnel to train in ways that optimize their ability to learn and be evaluated and maximize learning outcomes. This training significantly enhances team and organization readiness and resilience, and it can significantly reduce costs to the business. Research shows that organizations with an incident response (IR) team who regularly tested their IR plan experienced an average cost of a data breach that was USD 2 million lower, compared to organizations without an IR team or IR plan testing.[13]

3 Using Cyber Ranges to Build Practical Skills

Organizations can use cyber ranges in a variety of ways to strengthen their defenses and stay ahead of threat actors. There are several use cases for how organizations can leverage these capabilities.

Identifying skills gaps: Organizations can conduct assessments within a lab environment so cybersecurity experts can prove they have the skill sets required to protect against a specific vulnerability class. If gaps are identified, managers can ensure those individuals receive the customized, hands-on training they need to increase preparedness.

Developing skills and growing talent: Managers can train team members on new skills specific to the organization's cybersecurity needs. To ensure cybersecurity experts remain effective, cyber ranges can be used to continuously train and upskill a team. Managers can also use them for ongoing evaluation to ensure the right people are in the right roles, optimizing the effectiveness of the overall cybersecurity workforce.

Retaining existing talent: Organizations can help existing talent broaden their experience and expertise and develop the skills and credentials that make them more valuable in the market and to their employer. Cyber ranges can also be used to improve employee satisfaction, retention, and motivation by helping cybersecurity experts feel more prepared and empowered and by demonstrating commitment to their professional development.

Recruiting new talent: Certifications aren't everything. When hiring a new cybersecurity expert, managers can use cyber ranges to ensure without a doubt that a prospective recruit is competent and can demonstrate the skills required for the job.

Simulating Red Team/Blue Team exercises: Cyber ranges can be used to simulate real-world attack scenarios for Red and Blue teams to improve incident response capabilities. Red teams can think like adversaries trying to exploit weaknesses in the organization's cyber defenses, while Blue teams can focus on identifying and mitigating those attacks. The ability to play these war games in a simulated environment not only bolsters the teams' preparedness for a true cyber attack, but it also helps to expose security and compliance vulnerabilities so they can be quickly addressed.

Validating security controls and evaluating new tech: By simulating attack scenarios using cyber ranges, organizations can evaluate the effectiveness of their existing security controls, identify any weaknesses or gaps, and use outcomes to enhance security measures. Additionally cyber ranges can be used to assess viability and effectiveness of new cybersecurity technologies, tools, and solutions in a controlled environment before deploying them in production systems.

Re-enforcing incident response preparation: Cyber teams can use cyber ranges to continuously practice and fine-tune incident response procedures as new threats emerge, new technologies and techniques are implemented, new regulations are imposed, and business needs evolve.

4 Strengthening individuals, teams, and the organization

The benefits and value of using cyber ranges stretch across the entire organization. They can help upskill individual cybersecurity experts, strengthen team readiness, and fortify the organization's cybersecurity defenses.

1. Continually enhance skill development, competencies, and expertise

Teams can build practical skills, face challenges they would in a real-world engagement, and upskill faster so they can stay ahead of cyber attackers.

Cyber experts can become more versatile, adaptable, and valuable in their roles. Teams stay up to date on emerging cybersecurity technologies, threats and best practices. And organizations can continuously evaluate and train teams to iteratively enhance their defenses, responses, and skills over time.

2. Improve team communication and collaboration

The ability to safely simulate cybersecurity readiness exercises and rehearse incident response protocols help to optimize team collaboration and streamline communication during real cyber emergencies.

3. Validate compliance and policies

Organizations can validate security policies in a controlled environment and refine those policies to align with industry best practices and regulatory requirements to ensure the organization maintains compliance.

4. Enable collaborative learning and knowledge sharing

Organizations can take part in collaborative exercises with other entities like government agencies or industry partners, to share knowledge and strengthen collective cybersecurity capabilities. Doing so can help organization build valuable relationships and gain insights from diverse perspectives.

5 Conclusion

Research indicates that rapidly evolving cyber threats will only continue to grow in complexity, volume, and sophistication. Likewise, the consequences of a breach for today's businesses are increasingly severe and costly. Organizations must arm cybersecurity experts with the tools, knowledge, training, and hands-on experience to keep pace with the dynamic nature of cyber attacks. Cyber ranges prepare experts by moving beyond theoretical training to realistic, simulated environments where they can learn, test, and experience the pressure of real-world attacks within a safe environment. Organizations can also continuously reinforce cybersecurity defenses by using cyber range simulations to test new and existing technology, verify security controls, and ensure ongoing compliance. To learn more about how your organization can benefit from cyber range simulations, visit https://www.offsec.com/cyber-range/.

[1] https://venturebeat.com/security/report-average-time-to-detect-and-contain-a-breach-is-287-days/
[2] https://healthitsecurity.com/news/global-cyber attacks-increased-by-38-last-year-healthcare-hit-hard
[3] https://www.av-test.org/en/statistics/malware/
[4] https://www.forbes.com/sites/forbesbusinesscouncil/2023/02/09/welcome-to-2023-a-year-in-which-everyone-is-still-worried-about-ransomware/?sh=206c2f6f29f3
[5] https://www.darkreading.com/operations/identity-related-breaches-last-12-months
[6] https://securityboulevard.com/2023/01/what-happens-to-a-customer-after-a-data-breach/#:~:text=In%20the%20US%2C%2083%25%20of,to%20a%20business%20post%2Dbreach.
[7] https://www.ibm.com/reports/data-breach
[8] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
[9] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
[10] https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025
[11] https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyber attack-in-next-two-years/
[12] https://www.helpnetsecurity.com/2022/01/31/cybersecurity-teams-retention-issues/
[13] https://www.ibm.com/reports/data-breach