TAG

CYBER RANGE BUYER'S GUIDE

26 QUESTIONS TO ASK WHEN SELECTING A CYBER RANGE

CYBER RANGE BUYER'S GUIDE

26 QUESTIONS TO ASK WHEN SELECTING A CYBER RANGE

One of the most valuable resources of any modern enterprise is its security operations center (SOC) team. Tasked with guiding the day-to-day management of organizational cyber risk, team members in any SOC have the challenge to not only detect and respond to incidents, but also to keep up with the latest advances in technology, the latest innovations in cyber, and the most difficult shifts in how cyber threats are levied by malicious actors.

For this reason, there is strong motivation for SOC professionals and their management to take proactive steps to advance their technical and operational skills, both as individual members of the SOC team and as a combined group working together toward a common security goal. One of the most effective means for improving cyber readiness and validating operational performance for both individual practitioners and SOC teams involves the use of a cyber range.

This report provides a Buyer's Guide for practitioners and leaders who are seeking to increase their teams' readiness by partnering with a world-class provider of professional live-fire cyber range training. The guide explains the key functions that should be expected in any cyber range, as well as a long list of questions to ask during source selection to ensure that the cyber range under consideration has the right combination of support elements.

WHAT IS A CYBER RANGE?

A cyber range is a commercially offered cyber readiness environment that enables safe practice of defensive methods against cyberattacks. A cyber range uses live simulations of complex attacks to help SOC and cyber defense teams hone their skills, both as a team and as individuals. Companies such as Cloud Range provide these types of cyber range environments for commercial customers who value the goals of enhancing their SOC team's effectiveness and ensuring they are prepared to defend against an infinite number of threat vectors and attacks.

Cyber ranges are virtual, in the sense that they can flexibly simulate or incorporate key aspects of a live network environment. Cyber ranges can run in an isolated, standalone setup within a single enterprise or in a more expansive, globally accessible configuration. The interactive platforms in a robust cyber range generally include accurate commercial representations of networks and systems and incorporate licensed tools and applications to ensure a realistic environment that represents the production environments of the users.

Typical team-related objectives supported in a cyber range include ongoing and frequent preparation to defend against attacks identified through threat intelligence and public advisories, while reducing the skills gap for new and existing SOC staff. This supports a performance-based learning and assessment process, stimulating improved ways for individuals to work together as highly functional and well-communicating SOC teams, and providing real-time feedback for individuals in a dynamic environment where complex and novel situations can be simulated.

Modern cyber ranges are also evolving beyond training environments into platforms for validating operational readiness across both human teams and AI-driven systems. As AI becomes integrated into SOC workflows, threat detection pipelines, and response automation, organizations increasingly require safe environments where AI models and agentic security tools can be tested, trained, and evaluated under realistic adversarial conditions before being trusted in production operations. These validation ranges enable organizations to assess how AI models and agents detect threats, respond to attacks, and interact with enterprise security tools. The safe, controlled environment allows for easy measurement and refinement of the reliability, security, and operational readiness of AI-driven systems without experimenting in live environments or exposing real data.

The functions one finds in a cyber range such as from Cloud Range will include support for live-fire attack simulation exercises; incident response scenarios; red team, blue team, and purple team training; tabletop exercises; forensic analysis; capture the flag events; assessments of team candidates; runbook validation; threat intelligence simulation; product security testing; penetration testing; patch testing; vulnerability scanning; malware engineering; IT and OT convergence training; AI model validation and agent testing; and more.

WHAT TYPES OF ORGANIZATIONS USE CYBER RANGES?

In addition to supporting a wide range of professionals, cyber ranges scale well across many different types of organizations. In fact, it is challenging to find any type of organization that would not benefit from cyber range training. That said, the most common groups that are presently leveraging commercial cyber range solutions to assess, train, and continually upskill their SOC team performance include the following public and private entities:

1. **Commercial Enterprises** – Large organizations often face sophisticated cyber threats due to their size and the valuable data they possess. Cyber ranges allow them to conduct extensive security assessments, develop defense strategies against complex attack vectors, and provide advanced training for their cybersecurity teams. By simulating real-world attacks, large enterprises can test the resilience of their systems against potential breaches and refine their incident response strategies before actual threats materialize.

2. **Government and Military** – For government agencies and military organizations, the stakes are particularly high due to the sensitive nature of their data and the criticality of their operations. Cyber ranges in these sectors are used for highly specialized training that includes national security scenarios and defense against state-sponsored cyberattacks. These organizations benefit from cyber ranges by preparing their personnel for a wide array of threats, ensuring that they can respond swiftly and effectively to incidents that could have national implications.

3. **Critical Infrastructure** – Entities within sectors like energy, utilities, and transportation use cyber ranges to prepare for and mitigate risks associated with cyber-physical threats. Given their reliance on operational technology and industrial control systems, attack simulations are crucial for ensuring that staff can handle scenarios where both IT and OT environments are jeopardized. Training in cyber ranges helps safeguard essential services and ensures continuity of operations even during severe cyber incidents.

4. **Higher Education and Workforce Development** – Universities, colleges, and workforce development programs are increasingly using cyber ranges to provide students with hands-on experience in emulated enterprise environments before entering the cybersecurity workforce. Through live-fire simulations, labs, and team-based cyber defense exercises, students can apply classroom concepts in ways that better reflect real-world operational conditions and evolving industry needs.

Across these sectors, cyber ranges provide a controlled, safe environment to test and bolster cybersecurity defenses, experiment with new security procedures, hire and train personnel, gain real-world experience, test and showcase products, and refine playbooks. This proactive use is critical as it ensures that security teams are well prepared and skilled, thus reducing the potential impact of actual cyber threats.

WHY IS A CYBER RANGE NECESSARY?

To understand the value of a cyber range, it helps to review analogous uses of training to optimize key functions. For example, life safety teams develop simulations to mimic high-stakes situations where first responders must perform under pressure. Medical simulations use patient mannequins and virtual environments to teach emergency response. Even aerospace experts use flight simulators to replicate piloting under various conditions.

In the same way, security practitioners use cyber ranges and simulation platforms to develop the situational awareness and muscle memory required to respond effectively to cyberattacks before facing them in real-world operations. Cyber ranges create realistic, virtual environments where professionals can practice defending against sophisticated cyberattacks. Live-fire simulations on a cyber range are crucial for developing real-world, hands-on experience in a controlled, legal setting, mirroring the practical, high-fidelity training seen in other life safety fields.

Although still necessary for fundamental skill development, traditional training and certifications, as well as most incident response exercises, can sometimes be overly theoretical without much immersive, hands-on experience. Without real-world simulations, security teams need to wait for a real cyberattack to determine if they are prepared. Cyber ranges thus advance cybersecurity education, training, and certification, enabling teams to refine skills and accelerate their experience in a practical and safe manner.

As organizations operationalize AI within cybersecurity workflows, cyber ranges are also becoming important environments for validating how AI systems behave during simulated attacks, investigations, and response scenarios. This enables organizations to better understand operational reliability, decision-making behavior, and potential failure modes before AI systems are deployed into live security operations.

KEY QUESTIONS TO ASK WHEN SELECTING A CYBER RANGE

Navigating the world of cyber ranges can be challenging, especially when most ranges might initially seem the same. However, not all cyber ranges are created equal. As a result, it is helpful to review this set of key questions that can be used when selecting the best cyber range for one's application environment. These questions can be tuned to local conditions, but they should serve as a helpful base.

Comparing cyber ranges through a questioning process is valuable because many providers offer a framework for simulations, but will not include the necessary content, simulation exercises, tools, environments, assessments, labs, courses, metrics, or management. The customer must therefore manage the range, create content and simulations, troubleshoot any updates and compatibility issues, and determine how to report on usage and learning.

Another source selection issue is that some products referred to as a cyber range might include only one method of training, such as individual labs, educational courses, simulation exercises, or assessments. Also, some ranges might be linear or static and do not represent a full network environment. They may only display a handful of virtual machines that do not have live traffic or live attacks. These are useful for individual training but do not provide a multi-role, team environment reflective of how cyber defense is actually performed. Different platforms might also provide varying types of metrics, which might not be useful or actionable.

As a result, before any enterprise team decides on the selection of a commercially supported cyber range, we strongly recommend that they ask the following series of questions about the infrastructure, technology, content, and management support of that range. We offer these questions to help reduce the risk of selecting the wrong cyber range, which can result in lost time, effort, and money.

QUESTION 1. WHAT ENVIRONMENTS DOES THE CYBER RANGE INCLUDE?

When evaluating cyber ranges, it's crucial to consider the variety of available environments, including information technology, operational technology, and cloud infrastructures. Within those categories, there should be multiple network environment options, with each offering unique security challenges, such as data protection in IT, physical process control in OT, and secure configurations in cloud settings.

QUESTION 2. HOW CUSTOMIZABLE IS THE CYBER RANGE?

Features to consider include the ability to choose from or install custom or proprietary tools, the ability to modify traffic levels, and whether the difficulty of any provided simulations can be adjusted to challenge your team appropriately. Find out how the environments can be modified and if physical devices can be integrated via hardware in the loop. If you want your team to practice defending an environment that closely mirrors your own, determine if the cyber range can be customized to emulate your specific network infrastructure and toolset.

QUESTION 3. WHAT SYSTEMS AND TOOLS, IF ANY, ARE INCLUDED?

Some cyber ranges may include already integrated systems and software platforms such as application servers, database servers, email servers, switches, routers, SIEM platforms, firewalls, endpoint security systems, analysis tools, OT network monitoring systems, cloud security tools, and generative AI or machine learning systems. In advanced environments, the range may also support testing and validation of AI-driven SOC assistants, automated detection models, or agentic security workflows operating against simulated attacks. This is an important feature to ask about and include in cyber range source selection. If the tools you need are not already installed, find out the process to integrate them. Ideally, the range has a suite of pre-installed security tools for users to select from.

QUESTION 4. DOES THE RANGE SUPPORT VALIDATION AND TESTING OF AI SYSTEMS?

As artificial intelligence becomes embedded in security operations, organizations must ensure that AI models, AI agents, and automated workflows behave reliably under real attack conditions. A modern cyber range should allow organizations to safely test and evaluate AI-driven security tools, threat

detection models, SOC copilots, and agentic automation workflows before deployment into production environments. Buyers should ask whether the range supports adversarial testing of AI models and agents, validation of AI behavior under live-fire attack conditions, comparison of AI versus human analyst performance in identical scenarios, testing against malicious or manipulated inputs, and evaluation of how AI systems interact with enterprise security tools and operational workflows.

QUESTION 5. IS THE RANGE DELIVERED ON-PREMISES OR VIRTUALLY?

An on-premises cyber range is a physical facility equipped with dedicated hardware and software to simulate local network and security scenarios. It offers organizations full control over their cybersecurity training and testing environment, but the setup often involves upfront investment in infrastructure and maintenance. In contrast, a virtual cyber range is hosted online, allowing users to access the simulation environment remotely via the cloud. This approach minimizes hardware costs, offers greater scalability, and simplifies setup and updates.

QUESTION 6. WHAT SIMULATION CONTENT IS INCLUDED WITH THE CYBER RANGE?

If you want to use your cyber range to help train and upskill your team or to focus on reducing incident containment or incident remediation time, look for a platform that includes simulation content that your team can engage with. If you create your own content, then results or analysis could be skewed since there would be no third-party unbiased oversight.

The selected cyber range should offer diverse content options to suit various training needs including the following:

- **Live-Fire Team Simulations:** Real-time, dynamic exercises where teams collaboratively tackle simulated real-world cyberattacks, enhancing their experience, teamwork, decision-making, and practical skills under pressure. Live-fire simulations should include cyber defense, penetration testing, red team vs. blue team exercises, capture the flag events, and more.
- **Self-Paced Labs:** Modules that participants can complete at their own pace, or team members can complete in parallel, focusing on specific cybersecurity skills like network security or malware analysis, ideal for targeted learning and skill reinforcement.
- **Assessments:** Various tests, from quizzes to hands-on simulation challenges, assess participant knowledge and skills, helping identify strengths and areas for improvement. Evaluation of assessments should be defined locally, including keeping results private, so that team members can feel free to participate in simulations and labs where their skills might still be developing.

Ideally, buyers should look for a cyber range with a robust and growing content library that encompasses all these options to ensure comprehensive training, from theoretical understanding to practical application and teamwork in cybersecurity environments. Content must be constantly added to reflect current threat activity, advanced persistent threat groups, and related changes in the attack landscape.

QUESTION 7. HOW OFTEN IS THE CYBER RANGE UPDATED WITH NEW CONTENT?

This follow-up to the previous question is to ensure that the simulation library is not stagnant. Cyber threats evolve rapidly, so the cyber range's library should be updated regularly to reflect the current threat landscape, especially if it includes live-fire, team-based attack simulations. Also, buyers should ensure that there are varying degrees of difficulty within the simulation library to continue challenging the team as it grows and matures.

QUESTION 8. HOW IS THE EFFECTIVENESS OF THE CYBER RANGE INVESTMENT MEASURED?

It is essential for a cyber range simulation platform to provide detailed, actionable metrics and reporting that help organizations evaluate readiness, identify gaps, and measure improvement over time. Effective cyber range programs should move beyond simple completion tracking to provide operational insight into both individual and team performance under real-world attack conditions.

Organizations should look for metrics tied to technical performance, operational effectiveness, and behavioral readiness, including indicators such as time to detect, time to respond, escalation accuracy, incident coordination and leadership, IOC detection rates, decision quality, communication effectiveness, and response consistency across simulations. As organizations mature their programs, metrics should also demonstrate measurable improvement over time and help validate the effectiveness of training, workflows, tools, and operational processes.

Modern cyber range platforms should also provide visibility into tactics, techniques, and procedures aligned to frameworks such as MITRE ATT&CK, enabling organizations to better understand defensive coverage, identify gaps, and measure readiness against realistic adversary behaviors. Integrated dashboards and reporting should help security leaders track progress, benchmark performance, and generate meaningful operational insights that support broader cyber readiness objectives.

As organizations deploy AI-assisted security tools, cyber ranges can also be used to measure the performance of AI models and automated agents under realistic operational conditions. Metrics might include detection accuracy, escalation behavior, response consistency, false positives, unintended actions, and resilience against adversarial inputs. Understanding how AI systems perform during attack scenarios is becoming an increasingly important part of overall cyber readiness measurement.

QUESTION 9. DOES THE CYBER RANGE HAVE A TRADITIONAL OR GAMIFIED ENVIRONMENT, OR BOTH?

A gamified cyber range environment uses competition and rewards to boost engagement and learning in cybersecurity training. Pros include increased motivation and improved retention through rewards like points or badges, fostering teamwork and problem-solving skills. Cons involve the risk of focusing more on competition than learning, potentially overshadowing educational goals and discouraging less experienced participants. While gamification can make training more engaging, it must be carefully balanced to genuinely enhance skill development.

A traditional or standard cyber range environment focuses on straightforward skill development and scenario-based learning without integrating game-like elements such as points, badges, leaderboards, or competitive challenges. It typically emphasizes direct instruction and practice, prioritizing depth of knowledge and technical skills over engagement and entertainment. This approach is often more focused on conducting cybersecurity tasks and working in real-world environments to prepare participants for actual operational duties. If the goal is to prepare your team for cyber threats, a more traditional cyber range is ideal. Some cyber ranges provide the option to have either or to have a combination of both, such as realistic environments and simulations that are fun for teams and include badges.

QUESTION 10. DOES THE RANGE ENVIRONMENT REPRESENT AN ENTERPRISE NETWORK OR IS IT SIMPLY STATIC VMS?

This issue is related to the prior topic of whether live or static traffic is included in the range training and simulation environment. Buyers should determine if the selected range can simulate the specifics of a complex, hybrid enterprise, or if it is simply a series of virtual machines used for testing, which may not accurately reflect the complexity of real-world enterprise security operations.

This level of realism is especially important for validating AI systems and autonomous security workflows. Simplified or static environments may fail to accurately replicate how AI models and agents behave against real-world telemetry, network traffic, enterprise toolsets, and evolving attack conditions. Organizations evaluating AI-driven security operations should ensure the cyber range provides an environment capable of realistically simulating operational complexity.

QUESTION 11. IF THE RANGE SUPPORTS TEAM TRAINING, ARE THE USERS WORKING TOGETHER IN DIFFERENT ROLES, OR ARE THEY PERFORMING THE SAME TASKS IN PARALLEL?

This is a key consideration since no SOC team exists with all workers basically doing the same task, as in for example a university setting where students are taking a common exam. Realistic cyber range training should include workers performing complementary roles toward a targeted goal.

QUESTION 12. DOES THE RANGE HAVE LIVE TRAFFIC OR IS IT A STATIC ENVIRONMENT?

The use of live traffic versus static testing is an important option for practitioners selecting a good cyber range. In the best case, both options are available, and buyers should request information on this important feature before deciding on the range of choice.

QUESTION 13. WHAT PERSONNEL RESOURCES ARE NEEDED TO MANAGE AND MAINTAIN THE RANGE?

A live expert instructor enhances a dynamic simulation by providing real-time guidance, expertise, and feedback. Live instructors can tailor and adapt training to meet the team's needs, increasing relevance and challenge as needed. They also offer immediate clarifications and help troubleshoot issues, ensuring participants understand the rationale behind their actions. Some instructors will also score and analyze individual team members and the team as a whole throughout a simulation exercise, which provides deep and actionable insights to team leaders. Their presence in debriefing sessions further enriches learning, fosters a deeper understanding of cybersecurity principles, and makes the training more effective. Additionally, see if the cyber range platform includes a full support team that can assist with setup, configuration, customization, and simulation content, as well as range administration, coordination, and facilitation, ensuring teams meet their objectives.

QUESTION 14. DOES THE CYBER RANGE PROVIDER OFFER A CONTINUOUS TRAINING PROGRAM FOR CYBERSECURITY TEAMS, OR DO THEY ONLY CONDUCT ONE-OFF EVENTS?

Regularly engaging in live-fire simulations and lab exercises helps teams stay familiar with the growing threat landscape and cybersecurity tactics. This consistent practice enhances their ability to respond swiftly and effectively to real-world cyber threats, ensuring preparedness under pressure. As threats evolve, continuous simulation training allows teams to adapt their strategies, fostering a proactive rather than reactive security posture.

QUESTION 15. DO THE CYBER RANGE ATTACK SIMULATIONS ALIGN WITH INDUSTRY-STANDARD FRAMEWORKS?

Aligning a cyber range program with industry-standard frameworks like the MITRE ATT&CK Framework, the NIST NICE Workforce Framework for Cybersecurity, and the Department of Defense Cyber Workforce Framework ensures that training is relevant and comprehensive. Such alignment enhances the

program's credibility, making sure that participants develop the skills and knowledge recognized across the cybersecurity industry. It also supports standardized training approaches, facilitating the professional development and certification of cybersecurity personnel.

QUESTION 16. DOES THE CYBER RANGE INCLUDE MORE THAN ONE METHOD OF TRAINING, VERSUS JUST HAVING A SINGLE METHOD SUCH AS A LAB?

This is an important question to ask during source selection of a cyber range since many training environments will include just a simple common task to train all participants in a given cybersecurity method. Look for a cyber range platform that includes both live-fire, team-based attack simulations as well as individual skills development labs. Ideally, the provider will have additional training options as well, such as tabletop exercises, assessments, and other resources.

QUESTION 17. WHAT ADDITIONAL OPPORTUNITIES ARE AVAILABLE FOR TEAMS TO USE THE CYBER RANGE BEYOND SCHEDULED SIMULATIONS?

Having the cyber range available to an organization with 24/7/365 access allows team members to use it at any time to support ongoing operational testing, experimentation, and skills development. However, if the cyber range is purchased as part of a program, such as to access specific simulations, then free time on the range might not be available. Open range time can be beneficial for things like allowing a team to practice what they could not accomplish in a simulation, testing and refining playbooks, enabling red and blue teams to compete and test skills, reverse engineering malware, or deep diving into a vulnerability. A cyber range can also provide organizations with a safe environment to test AI-assisted workflows, evaluate autonomous agents, experiment with operational guardrails, and validate how AI systems behave during simulated attacks without impacting production operations. It's good to understand the options since it may impact a SOC team's training accessibility and convenience.

QUESTION 18. DOES THE CYBER RANGE OFFER THE ABILITY TO GENERATE CUSTOM LEARNING PLANS?

Customized learning plans are vital for cybersecurity teams as they address the specific strengths, weaknesses, and roles of each member. This personalized approach ensures targeted skill development and maximizes training effectiveness, enhancing motivation and engagement. Consequently, these tailored plans help build a more competent and responsive team, better equipped to tackle evolving cybersecurity challenges. The best custom learning plans are integrated into the overall mission of the organization and include coordination points with all training activities being delivered.

QUESTION 19. DOES THE CYBER RANGE PROVIDE A SINGLE POINT OF ACCESS FOR ALL CONTENT, RANGE ADMINISTRATION, AND REPORTING?

Having a single point of access for the cyber range streamlines the management and usage of the system, greatly enhancing efficiency and user experience. This consolidation simplifies the navigation of training modules, the execution of simulations, and the analysis of performance data, making it easier for users to access resources and for administrators to oversee operations and generate reports. It reduces complexity and saves time, allowing both learners and instructors to focus more on the educational aspects rather than on logistical challenges. Additionally, a unified access point minimizes the risk of security gaps, ensuring a secure and effective training environment.

QUESTION 20. WHAT KIND OF ONGOING SUPPORT DOES THE CYBER RANGE VENDOR OFFER?

When selecting a cyber range, it's crucial to consider the quality of technical support, troubleshooting capabilities, and the frequency and reliability of updates. Effective technical support ensures that any issues encountered during training can be quickly addressed, minimizing downtime and maximizing learning continuity. Responsive troubleshooting and support personnel are essential for resolving technical problems efficiently. Regular updates are also important, as they keep the cyber range's environments, tools, simulations, and security measures up to date with the latest cybersecurity threats and technologies. Ensuring these aspects are well-covered will contribute to a smoother, more effective training experience and better long-term value from the cyber range.

QUESTION 21. IS THE CYBER RANGE VENDOR EXPERIENCED AND REPUTABLE?

It's important to understand the track record of the vendor in providing robust and effective cyber range solutions. How recognized is it in the industry? Can references be obtained from current and former customers? Are there reviews you can read? Is their sales team applying high-pressure tactics? This is a long-term investment, so due diligence is necessary to ensure a successful partnership.

QUESTION 22. HOW DOES PRICING WORK?

Do you understand the pricing on the front end, or could there be surprise invoices later? Beyond the purchase price, consider potential future costs like updates, support, and additional hardware or software. Will you need to make any adjustments in your own environment or team to accommodate the cyber range?

QUESTION 23. HOW CAN THE INVESTMENT BE JUSTIFIED TO PRIORITIZE BUDGET?

The return on investment for range training can be viewed in the context of both qualitative improvements in SOC team performance, such as time to detect and time to respond, communications, and coordination, as well as quantitative improvements in the CISO budget usually stemming from greatly reduced likelihood of having to budget for expensive incident response tasks. Buyers of cyber range solutions should request a full return on investment or value analysis from prospective providers. Buyers should also evaluate how cyber range metrics and reporting can help demonstrate measurable improvements in cyber readiness and operational performance over time.

QUESTION 24. DOES THE SIMULATION CONTENT COME WITH CPE CREDIT?

Providing continuing professional education credits for cyber range simulations and labs adds significant value, allowing participants to simultaneously enhance their cybersecurity skills and meet professional development requirements. This makes cyber range training an attractive and practical choice for continuous learning and certification maintenance, thereby encouraging ongoing professional growth and compliance with industry standards.

QUESTION 25. WHAT IS THE SCALABILITY OF THE CYBER RANGE?

Scalability is crucial for cyber ranges, ensuring they can accommodate an increasing number of users and more complex simulations and scenarios as organizational needs grow. A scalable cyber range adapts to technological advancements and expanding training requirements, allowing for continuous cybersecurity education and defense capability enhancement without performance loss. This adaptability is essential to keep pace with the dynamic nature of threats.

QUESTION 26. WHAT OTHER USES ARE THERE FOR A CYBER RANGE?

Ask your proposed cyber range vendor to share their experiences of how customers are using cyber range platforms beyond traditional team simulations and skills development. Modern cyber ranges are being used for incident response exercises, tabletop exercises, hiring assessments, sandbox testing, product integration testing, workflow and runbook testing, generation of novel metrics, AI system validation, and more.

Organizations may also use cyber ranges to safely evaluate emerging technologies, validate detection and response workflows, test security tool effectiveness, refine escalation procedures, and measure performance improvements over time under realistic attack conditions. These broader use cases help organizations maximize the long-term operational value of the platform beyond periodic training events.

THE CLOUD RANGE DIFFERENTIATION

Commercial vendor Cloud Range should be included in all source selection processes for cyber range solutions. In addition to lining up closely with the set of criteria implied by the questions listed above, we can offer some additional insights below into why Cloud Range is such a desirable partner for any enterprise or government teams, as well as higher education institutions, desiring a means for improving the effectiveness of their SOC team and staff. Key value propositions for Cloud Range include the following:

- **Blue Team Exercises:** Cyber defense teams focus on detecting, responding to, and remediating live attacks, testing their ability to defend against various real-world threats. Cloud Range's library of dynamic attack scenarios can be used to simulate a range of adversary tactics, from network breaches to malware infections.
- **Red Team vs. Blue Team Exercises:** Cloud Range enables competitive and collaborative exercises where one team instigates an attack while another team defends. These exercises help your team understand the tactics and strategies used by adversaries and how to counter them in real time.
- **Purple Team Exercises:** Purple team training fosters collaboration between the offensive and defensive teams, promoting shared insights and improved coordination to enhance overall security posture.
- **AI Validation and Agentic Security Testing:** Organizations can safely test, train, validate, and benchmark AI models, AI-powered SOC assistants, and agentic security systems under realistic cyber attack conditions. Cloud Range enables evaluation of AI behavior, operational reliability, escalation logic, adversarial resilience, and human versus AI performance before deployment into production security operations.
- **Tabletop 2.0 Exercises:** Cloud Range's advanced, simulation-supported tabletop offering includes the option to integrate live-fire simulation into tabletop exercises, providing both technical and non-technical participants a comprehensive view of threat detection, response, and remediation. This allows leadership and stakeholders to validate incident response plans in a real-world setting.
- **Sandbox Testing:** Use the cyber range as a sandbox to safely test new technologies, run malware analysis, or simulate specific situations without risking your live network. This enables your team to evaluate potential risks, vulnerabilities, and the impact of new technologies.
- **Product Integration Testing:** Evaluate how new tools or solutions will integrate into your existing security environment. With the ability to replicate your IT, OT, and cloud network, the cyber range allows seamless testing of integrations before deploying them in a live environment.

- **Capture the Flag Exercises:** Teams can participate in fun, competitive capture the flag exercises where they are tasked with solving cybersecurity challenges, such as finding hidden clues or flags.
- **Runbook Validation:** Test and validate your organization's incident response playbooks in a controlled environment, ensuring that your processes and procedures are well-established and effective in the event of a real attack.
- **Candidate Assessments:** Cloud Range's aptitude and hiring assessments enable you to evaluate potential hires with simulation-based exercises that test their abilities, knowledge, and practical skills in real-world situations. These assessments can be tailored to specific roles, allowing you to identify top talent and make data-driven hiring decisions.
- **Product Demonstrations:** Showcase the capabilities of cybersecurity tools and solutions in a realistic, simulated environment without impacting your environment. Cloud Range's cyber range platform enables vendors and teams to demonstrate product value and performance under live-fire attack scenarios to stakeholders and decision-makers.
- **Technology Testing:** Evaluate and stress-test emerging technologies in a controlled environment before deploying them in production. Cloud Range supports testing for firewalls, SIEMs, IDS and IPS systems, and other tools to identify potential gaps or conflicts.
- **IT and OT Convergence Exercises:** Conduct specialized training scenarios that replicate the challenges of integrating IT and OT environments. Cloud Range supports the development of strategies for securing converged networks while addressing unique threats to industrial control systems.
- **Penetration Testing Simulations:** Utilize the range to safely perform penetration testing exercises, replicating adversarial tactics, techniques, and procedures to uncover vulnerabilities without disrupting live environments.
- **Forensic Analysis:** Practice advanced forensic skills in a controlled environment. Cloud Range enables teams to investigate a variety of simulated breaches, analyze logs, and identify the root cause of incidents to enhance investigative and incident response capabilities.

Additional capabilities that differentiate Cloud Range from any other means for improving the effectiveness of a security operations team include the following:

FULLY HOSTED, CLOUD-BASED RANGE PLATFORM

From the target network environment, enterprise architecture, and deployed tools to the attack type, traffic generation, and complexity level, Cloud Range's professional cyber ranges are fully hosted and managed. The safe, production-like enterprise network and SOC environment includes licensed SIEMs, firewalls, endpoint tools, and numerous other integrated security technologies. Its full-service model also includes program management, facilitation, coordination, and reporting, helping organizations maintain cyber readiness without the operational burden of managing range infrastructure internally.

In addition to standard IT environments, Cloud Range's optional operational technology (OT) and industrial control system (ICS) environments also include virtualized programmable logic controllers, human-machine interfaces, monitoring tools, and hardware-in-the-loop capabilities. The range combines realistic enterprise environments, integrated security tools, expert-developed simulations, and measurable reporting on a single platform.

CYBER ATTACK SIMULATION CONTENT LIBRARY

While many cyber ranges require practitioners to build scenarios, Cloud Range has a regularly growing library of live-fire attack simulations for teams based on real threat intelligence and mapped to the MITRE ATT&CK and other industry-standard frameworks. Scenarios include ransomware, OT and ICS attacks, distributed denial of service attacks, phishing, domain name system tunneling, website defacement, supply chain attacks, and more.

MULTIPLE LEARNING FORMATS

Cloud Range's thousands of simulation options include red, blue, red vs. blue, and purple team training exercises, capture the flag events, skill development and challenge labs, and next-generation tabletop exercises.

INSTRUCTOR-LED SESSIONS

Expert Attackmasters provide live counsel throughout live-fire team-based simulations, ensure interaction and engagement, and evaluate performance and skills.

OT AND ICS COMPONENTS

Cloud Range has the only virtual live-fire OT and ICS cyber range for team training and regularly develops new cyberattack simulations. That enables OT incident response and ICS security teams to be immersed in and understand various attack flows, vulnerable ingress points, how to respond if a system is compromised, and how to limit cyber-physical damage.

AI VALIDATION RANGE

Cloud Range has expanded the traditional cyber range concept by introducing the AI Validation Range, which enables organizations to test, train, and validate artificial intelligence models and agentic security systems before deployment. In this controlled environment, AI models and agents can be exposed to realistic adversarial scenarios, enabling organizations to observe how they detect threats, respond to malicious activity, and interact with enterprise security tools. The platform allows security leaders to measure AI reliability, identify failure modes, and establish operational guardrails before AI systems are integrated into production security operations. This approach helps organizations adopt AI in the SOC with greater confidence while reducing the risk associated with deploying untested automated decision systems.

PERFORMANCE EVALUATION AND REPORTING

All progress is tracked in an integrated learning management system with scoring and analysis that factor in tasks, knowledge, and skills statements from the NICE Framework, tactics, techniques, and procedures from MITRE ATT&CK frameworks, industry-specific regulations, job requirements, technical proficiencies, soft skills, and mean and actual time to detection. Customized learning plans can be easily generated based on each person's goals, roles, assessments, and organizational criteria. Cloud Range provides metrics and detailed analysis of individual and team performance, so security leaders can track changes and improvement over time, which directly translates to decreased levels of cyber risk. Additional metrics include IOC detection rates, MITRE ATT&CK-aligned visibility into adversary coverage, incident leadership and coordination, and operational performance trends over time. As organizations integrate AI-driven security operations, reporting can also provide visibility into AI system behavior, response consistency, and decision quality under attack conditions.

SUMMARY

Cloud Range's cyber readiness and validation platform enables organizations to measure, improve, and validate cyber defense performance through realistic attack simulations, operational testing, actionable metrics, and hands-on exercises across human teams and AI-driven systems.

Modern cyber ranges are evolving beyond environments used solely for training activities into platforms that help organizations validate operational readiness under real-world conditions. As cyber threats continue to evolve and AI becomes integrated into security operations, organizations increasingly require measurable ways to evaluate how people, processes, tools, and automated systems perform during real-world attack scenarios.

Cloud Range enables organizations to safely test and evaluate cyber defense capabilities across IT, OT, cloud, and hybrid enterprise environments using live-fire attack simulations, enterprise telemetry, operational performance analysis, and integrated readiness measurement. Organizations can validate incident response workflows, benchmark team and AI performance, identify operational gaps, and measure improvement over time within adversarial conditions.

Beyond training human defenders, modern cyber ranges are also becoming important environments for validating AI models, AI-powered SOC assistants, and agentic security systems before deployment into production operations. Cloud Range's AI Validation Range enables organizations to observe how AI systems behave during realistic attacks, investigations, and response scenarios, helping establish operational confidence while reducing the risks associated with deploying untested automated systems.

Security leaders and teams are drawn to Cloud Range's platform because it helps organizations establish measurable cyber readiness, strengthen resilience, validate operational performance, and reduce the organization's exposure to evolving cyber threats.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.