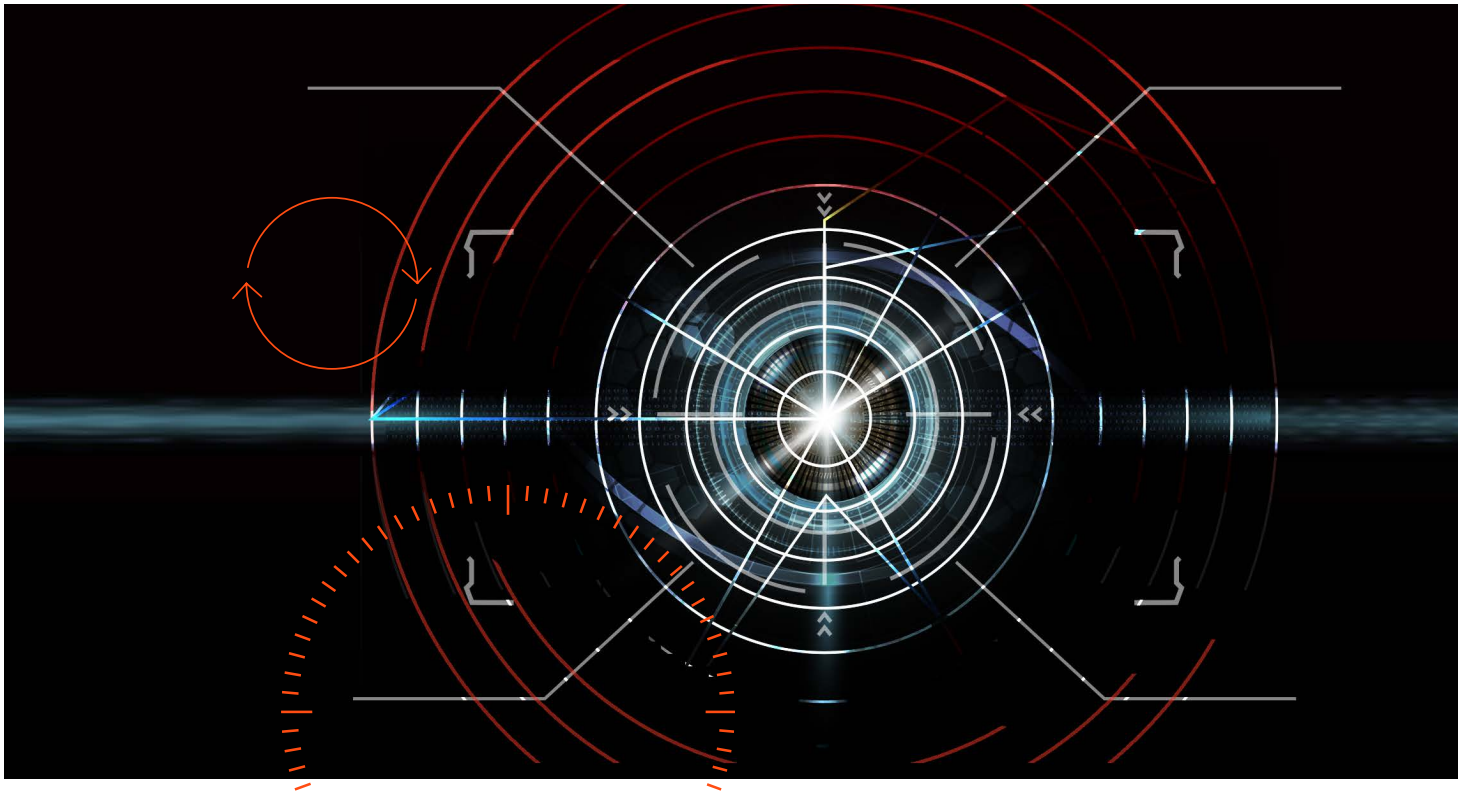
SIMSPACE

whitepaper



THE COMPREHENSIVE GUIDE TO CYBER RANGES

SIMSPACE
SECURE WITH CONFIDENCE

contents

- What is a cyber range? 5
- Why do organizations use cyber ranges? 7
- What are the different cyber range delivery models? 13
- How does a cyber range simulation work? 15
- What makes the SimSpace cyber range the right choice? 18

From an often ignored IT issue to becoming a boardroom priority, the role of cybersecurity has changed dramatically in the past few years. In the wake of high-profile data breaches, increased regulatory, compliance, and cyber insurance requirements—and the brand damage impact on company valuation—it's no wonder the game has changed.

In most cases, good cybersecurity can avoid these issues and lower the cost of cyber insurance premiums for organizations that can demonstrate and quantify security teams' capabilities, processes, and technology.

For these reasons and more, business leaders and security professionals are looking for every advantage they can get when securing their brand reputations and their customers' data.

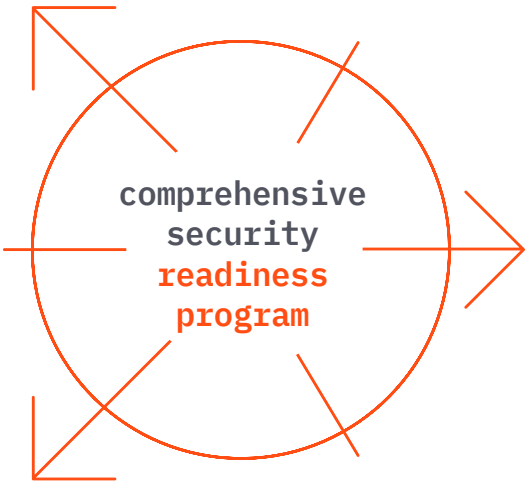
the game has changed

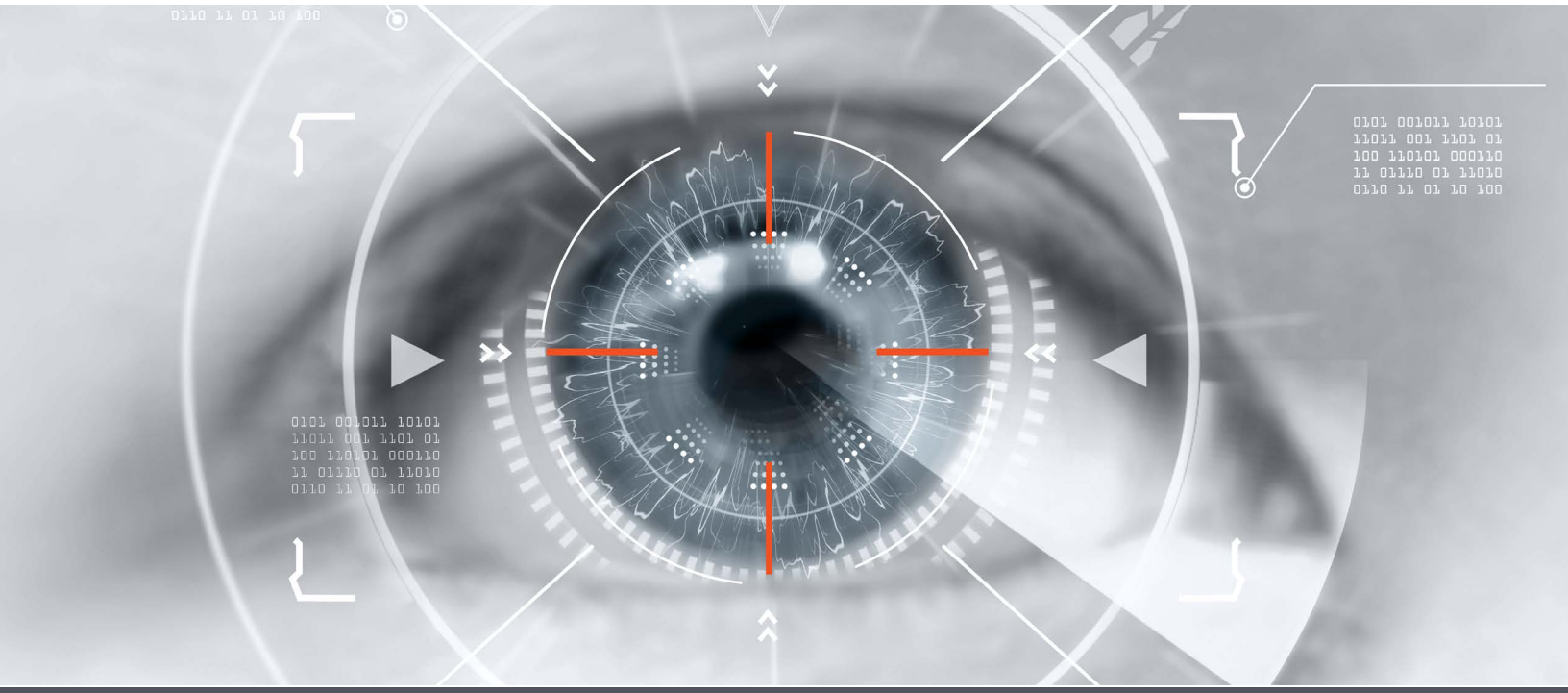
There are undoubtedly many tools, best practices, and training programs that organizations can use to improve their security posture, optimize their technology stack, and dial in their incident response. Each of these security components must work in harmony, to achieve the results security professionals and organizations require to react effectively to real world threat events.

Fortunately, as threats have evolved, so have the resources available for organizations to fight back.

One of the most efficient and cost-effective ways to optimize your security teams and overall security posture is integrating a cyber range into a comprehensive security readiness program. But just what is a cyber range and how can your organization use it to your advantage?

Business leaders and security professionals are looking for every advantage they can get when securing their brand reputations and their customers' data.





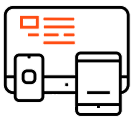
What Is a Cyber Range?

Cyber ranges are high-fidelity, simulated environments where security professionals can train, test, and practice responding to different security scenarios and experiment with security configurations, tools, and products to adjust to the latest security attacks. For example, cyber ranges are currently being used to:

- **Test** security stacks and configurations.
- **Provide** live attack scenarios to train and assess teams and individuals.
- **Provide** evidence for compliance with regulatory requirements and security frameworks.
- **Synchronize** incident response across people, processes, and technology.
- **Help** security vendors test and develop new products.

A cyber range is made up of a platform that creates a high-fidelity clone of production IT and OT environments, including:

Servers



Applications

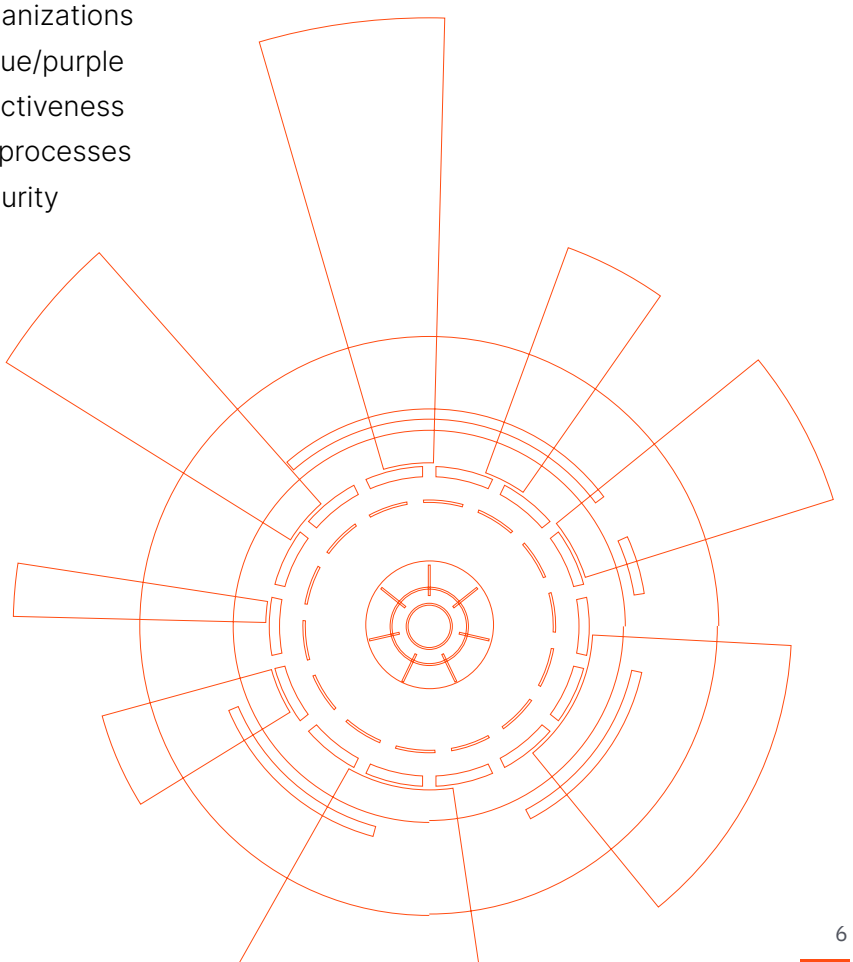
Cloud instances and servers

Networking and IoT devices

Securtiy stack products

Open-source tools

A fully configured cyber range allows organizations to deploy specific and measurable red/blue/purple team training scenarios, validate the effectiveness of their security stack, and confirm their processes will be capable of repelling the latest security requirements and ensure compliance.



Why do organizations use cyber ranges?

The simple reason that organizations deploy ranges is to increase, quantify, and validate cyber readiness and provide evidence of compliance for a wide variety of regulatory demands. Cyber ranges deploy a selection of testing and training capabilities to enable your security, risk, and vendor management teams to meet the objectives of your business or mission. From helping your team evaluate new tools to measuring staff readiness to pitting your defenses against specific attack scenarios, cyber ranges can be molded to fit your organization's exact objectives and reporting requirements.

Increase enterprise readiness.

As any security leader knows, all employees across an enterprise must participate in maintaining cybersecurity. Modern cyber ranges can help with these learning and development situations, too.

In fact, simulations can be tailored to fit any industry's operational environment and be used as part of larger organizational training exercises. For example, executives can practice how they handle media relations, interactions with law enforcement, internal communications, key technical decisions, and business risks.

In other situations, employees in other functions, such as finance or human resources, can practice how they would respond to phishing emails or updates from security team members to help thwart an attempted attack.

The lessons learned from these simulations can allow your organization to improve how your business units, managers, and security teams respond to attacks in a coordinated way.

Simulations can be tailored to fit any industry's operational environment and be used as part of larger organizational training exercises.

Optimize security processes and technology stack.

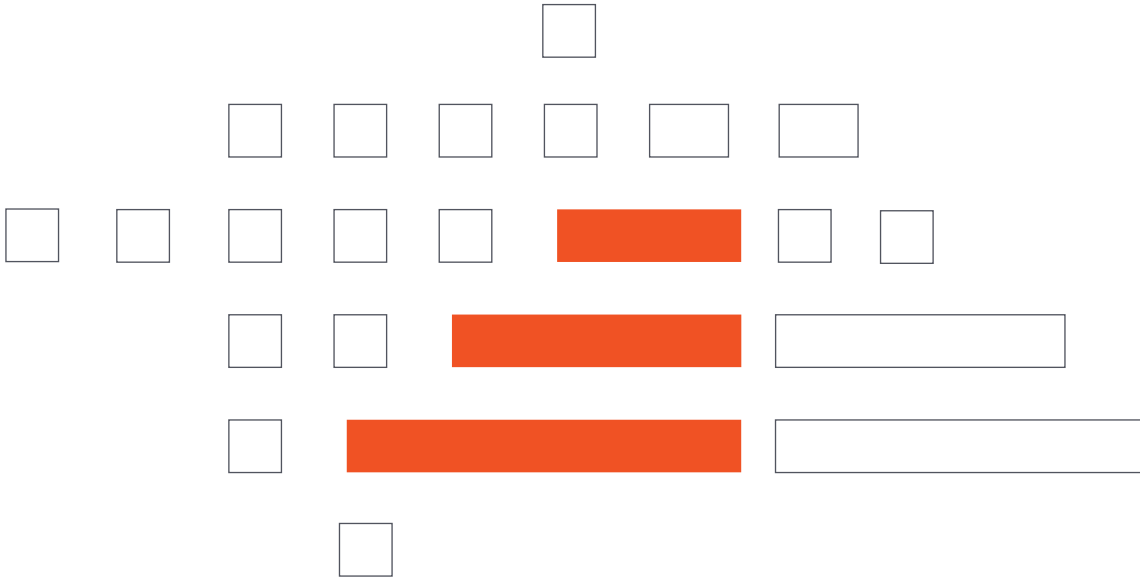
Sometimes building and validating a security stack can feel like strategically stacking slices of Swiss cheese and hoping you've covered all the holes. Cyber ranges allow you to test, adjust, stress, and validate your security stack and your existing incident response plans, thereby creating a higher level of security readiness.

To start, organizations can stress-test how existing defenses in their current network environment withstand the pressure of a real attack, how quickly incident detection systems are triggered, and what responses your team initiate. In other situations, an organization can build on its setup with minor modifications or major changes to test how its attack surface changes.

Evaluate Security Stacks.

One of the most crucial responsibilities for every security team is choosing which products will make up their organization's security stack.

The decision to invest in and deploy a new security tool can be complex and have many known and unknown downstream impacts. Advanced cyber ranges give your security team the ability to evaluate products, test new patches before they go into production, and monitor them during operation. Cyber ranges give you the ability to know how they will perform and interact with the rest of your current security portfolio attacks in a coordinated way.

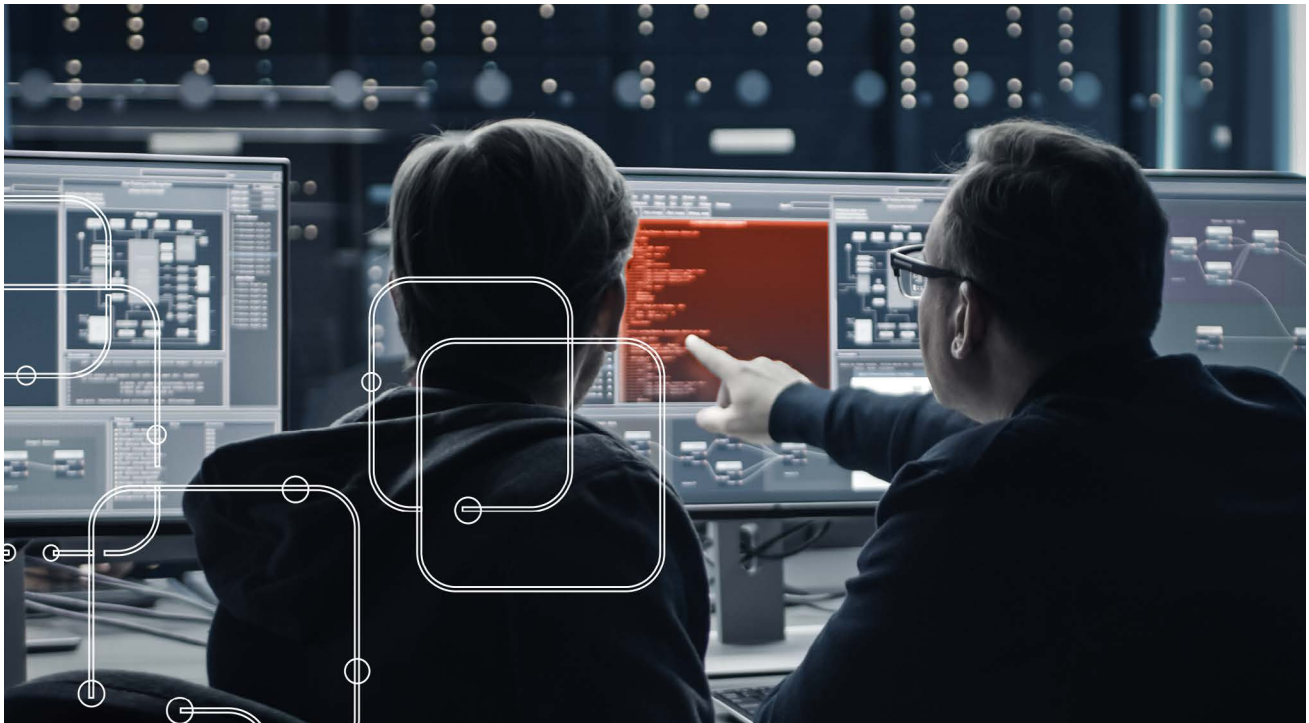


Instead of discovering issues after you buy a new tool, you can test out the product in the safety of a cyber range instead of your live environment—all before you buy.

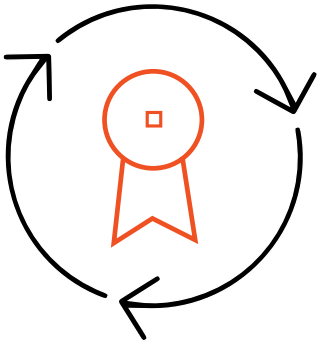
Replicate attack scenarios.

Cyber ranges allow your organization to simulate any cyberattack scenario your infrastructure can face. In these simulations, security professionals can fully practice their incident response playbooks and go beyond gamification exercises to see how they react when faced with a real threat. As cyber range events continue to evolve, your team can immediately apply what they have learned, refine the configurations of their security tools and response protocols, and improve response plans until your incident response team is as ready as it can be.

Cyber ranges allow your organization to simulate any cyber attack scenario your infrastructure can face.



Provide evidence for compliance.



There are thousands of regulatory and compliance requirements for organizations to follow. They tend to be in four groups:

General

From the ubiquitous SOC 2 report for public companies to requirements for publicly traded businesses and even those required of government agencies and educational institutions, an organization must prove that basic security capabilities and best practices are in place.

Data Privacy

Across the globe, GDPR, CPPA, CCPA, and many others set strict standards for data privacy and user control of data. To comply with these requirements, organizations must have stringent security practices and data management processes in place.

Operational and VRM

The most common examples are ISO 27001 and the U.S. Department of Defense's CMMC. These and other operational and supply chain standards require that security teams have their security model independently assessed to prove that they can meet the requirements to be a vendor.

Industry-Specific

Each industry has its specific compliance requirements that govern how businesses secure and manage data as well as system and network access. For example, financial firms must support PCI DSS and FFIEC, while healthcare organizations must comply with HIPAA and HITRUST.

Cyber ranges provide a comprehensive method to validate that you can meet these requirements.

Provide analytics and reporting required for security measurement.

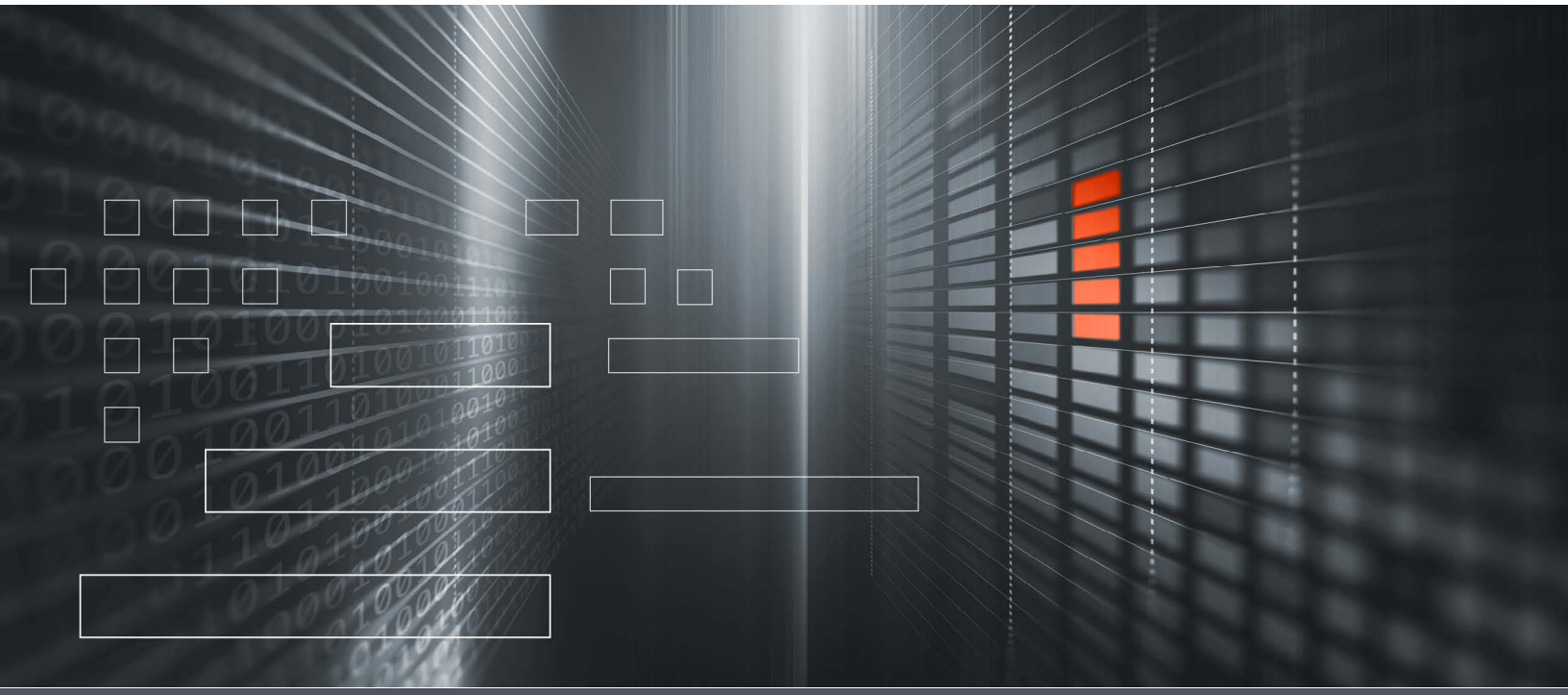
All security leaders have to report on the state of their security programs, including the people, processes, and technology involved. Sometimes, this is in deep analytics using tools like Splunk, or workforces readiness tools like Workday, or high-level reports for executives and board members.

Evaluate potential hires.

Formal training and certifications in cybersecurity, networking, and computer science provide a solid foundation for any security professional, but organizations often need their new hire to hit the ground running. Cyber ranges are the perfect proving ground for these purposes.

For example, you can build candidate assessments that present different scenarios in a cyber range to evaluate how an applicant reacts, measure their skillset in different security or networking tools, or see how well they can communicate technical topics in operational terms.

You can also use cyber ranges to evaluate your existing team's strengths and weaknesses in different technical domains. You can then use the results to create personalized training plans for continuous improvement and professional development.



What are the different cyber range delivery models?

As with other technology solutions today, organizations have options when it comes to how they can create, manage, and leverage their cyber range.

Based on its budget, its training and testing needs, and the resources it has available to administer a cyber range, an organization can choose either an on-premises deployment or one that is cloud-based.

An organization can choose either an on-premises deployment or one that is cloud-based.

A cloud-hosted cyber range provides flexible, easily reconfigurable, and cost-effective infrastructure for organizations that need it.

On-Premises Deployment

On-premises implementations give organizations the ability to create and use a cyber range exactly as they choose. Whether by using their own equipment and technology to design a cyber range or by leveraging a cyber range platform provided by a leading industry provider, organizations can segregate their cyber range training and testing environments in their own private cloud or in-house hosted infrastructure.

The administration of an on-premises deployment can be more complex, but the security of knowing the cyber range is hosted internally (or even completely air-gapped) can be worth it.

Cloud-Based Deployment

Like other as-a-service offerings, a cloud-hosted cyber range provides flexible, easily reconfigurable, and cost-effective infrastructure for organizations that need it, without all of the responsibility for management and maintenance put on internal staff.

Choosing this model means having access to advanced training and testing environments in an isolated, safe, and controlled environment that is scalable based on needs and budget.

Similarly, an organization can choose to host its cyber range in an existing cloud infrastructure, deploying and managing it like other on-demand services.

How does a cyber range simulation work?

The great thing about a cyber range is that it can be set up, used, reset, and rerun as many times and in as many different configurations as needed, all while keeping your production systems safe.

Every scenario or simulation will be different, but the lifecycle of a cyber range simulation generally follows a set pattern.

Common steps include:

Establishing objectives:

Whether it is a one-off training event, a candidate evaluation, or a simulation, establishing the objectives for the exercise is vital for identifying the people, processes, technology, and analytics required to measure success and prepare the environment.

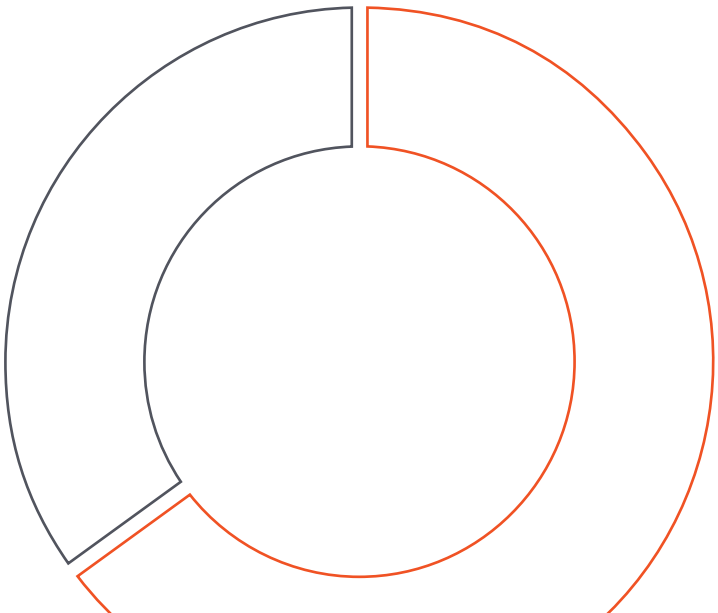
Building out the infrastructure:

Based on the goals and objectives established, identify the number and type of servers and clients needed, the security tools to deploy, and the interfaces and networking to accurately create the cyber range environment.

At this stage, partnering with a trusted cyber range provider can make the process more efficient. Your team can select from a number of pre-existing scenarios, which include the defensive and offensive elements of the exercise as well as simulated "regular" network activity.

Configuration:

Next, security tools, clients, servers, and network devices are configured to match the requirements of the scenario, which could include replication of an actual production environment or one that is slightly modified to test the impact of certain changes.



Documenting and measuring results:

Once the scenario is underway, documentation of key actions, outcomes, and events is key to conducting a productive debrief of the event. These key lessons learned and areas for improvement can be used for the next phase of training or evaluation.

Or, in the case of a candidate assessment, the results of the cyber range scenario can be joined with other elements of the interview process to help organizations make a more informed decision.

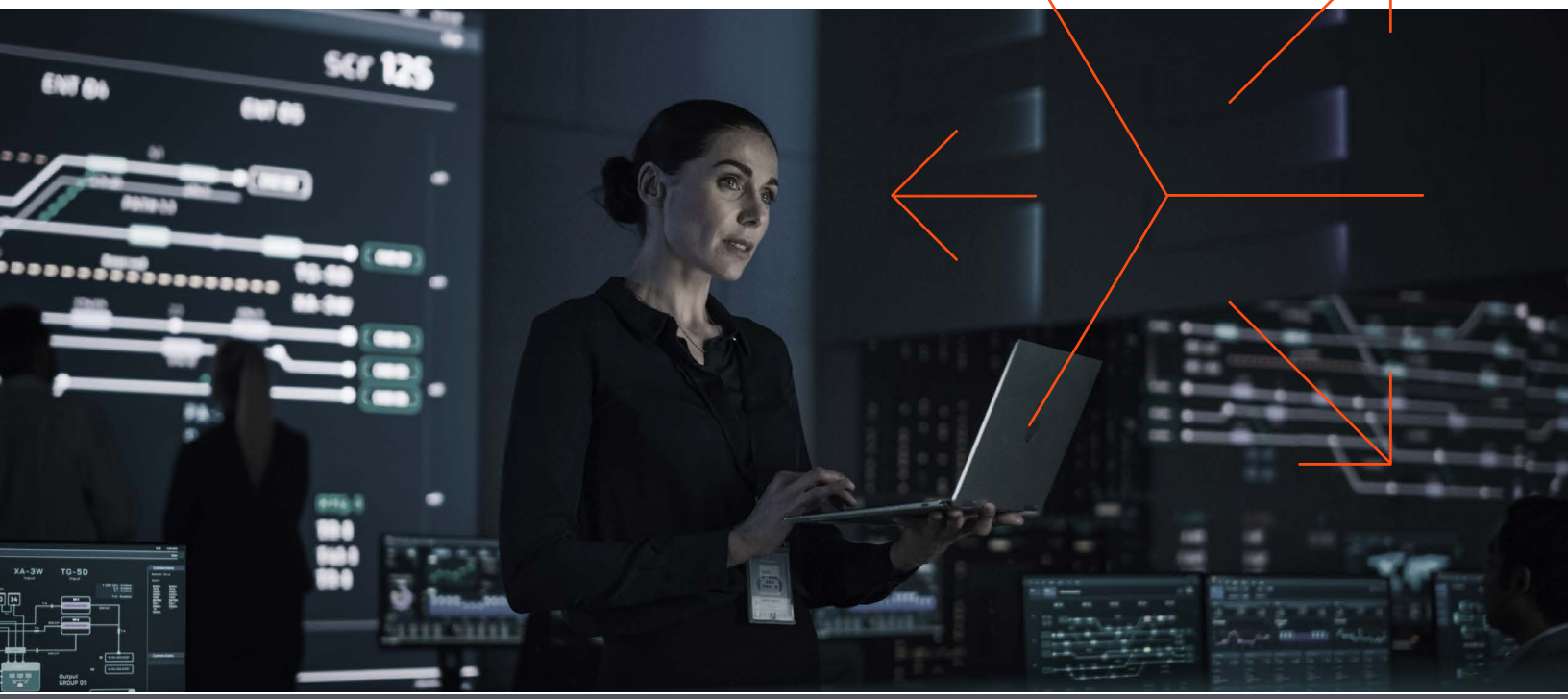
Resetting and repeating:

A key capability of a cyber range is its versatility. As soon as the cyber range event is done, teams can shut off specific virtualized systems, change configurations, and deploy new scenarios quickly and easily. This allows teams to refine their responses or ramp up the pressure for continuous improvement.

Prepping the scenario:

This involves preparing the cyber range event participants for the scenario they are about to be a part of and the attack or test cases. For example, this could include loading up the elements needed to replicate a(n):

- Malware attack
- Natural weather event
- Distributed denial of service (DDoS) attack
- Insider threat
- Ransomware attack
- Training scenarios or cyber range evaluations
- Advanced persistent threat (APT) situation
- Red team versus blue team challenge
- Blended purple team training scenario



What makes the SimSpace cyber range the right choice?

Throughout this guide, we have highlighted numerous benefits that cyber ranges can deliver for security teams of all sizes, locations, industries, and skill levels.

However, in order to maximize their training time and financial investment, many organizations choose to partner with a cyber range provider that can expedite the delivery of the range environment and introduce a wide range of existing scenarios.

This has been the case for numerous public and private sector organizations, including the Department of Defense and global banking institutions, that have chosen SimSpace to deliver cyber attack simulations and exercises and training curricula for all skill levels. SimSpace even has an established candidate assessment module to help organizations improve their hiring decisions.

SimSpace can deliver prebuilt, high-fidelity ranges that cover both IT and OT attack surfaces in both cloud and on-premises infrastructure, paired with a long list of available network and security tools with which to build infrastructure scenarios. SimSpace can also initiate automated, MITRE-inspired attacks powered by artificial intelligence and machine learning to more closely replicate real and APT attacks as well as end-user emulations.

Finally, SimSpace has logging and sensor technology deployed throughout its cyber range infrastructure to aid in providing detailed analytics and quantitative data, individual and team assessments, and actionable intelligence for teams, technology, and processes. This same technology can also be used to help teams evaluate different security tool deployments and configurations before they either make the full investment or take the time to test and deploy the systems in their production environments.

This information can be used to pinpoint development areas, highlight key turning points in network defense, and monitor progress overtime.

SimSpace even has an established candidate assessment module to help organizations improve their hiring decisions.

SimSpace can deliver your organization a proven cyber range platform

The contents of this guide only begin to scratch the surface of what your organization can get out of these powerful simulation and training environments.

If your organization wants to not only get the most out of your experience with cyber ranges but also maximize the training and testing needed to take your cybersecurity to the next level, then the decision to partner with SimSpace is an obvious choice.

SimSpace can deliver your organization a proven cyber range platform and the training scenarios your team needs to be at the top of its game and maintain its edge. This is especially vital today because continuing to utilize the same techniques and training methods in the face of ever-evolving cyber threats is not going to be enough anymore.

The SimSpace cyber range allows your team to go beyond just deploying enterprise and endpoint monitoring tools and leaning on incident response plans. Instead, you can take the hands-on actions required to form the team bonds and muscle memory needed to be ready to respond to a real cyber threat event.

Is your organization ready to take the next step? Then the team at SimSpace would welcome the chance to meet with you and set up your own personalized demonstration of the SimSpace cyber range platform.