DATASHEET

SIMSPACE

SIMSPACE CYBER RISK ASSESSMENTS

- TEAM EVALUATION
- CONTINUOUS IMPROVEMENT
- OBJECTIVE PERFORMANCE DATA

CYBER RISK ASSESSMSENTS

SIMSPACE
SECURE WITH CONFIDENCE

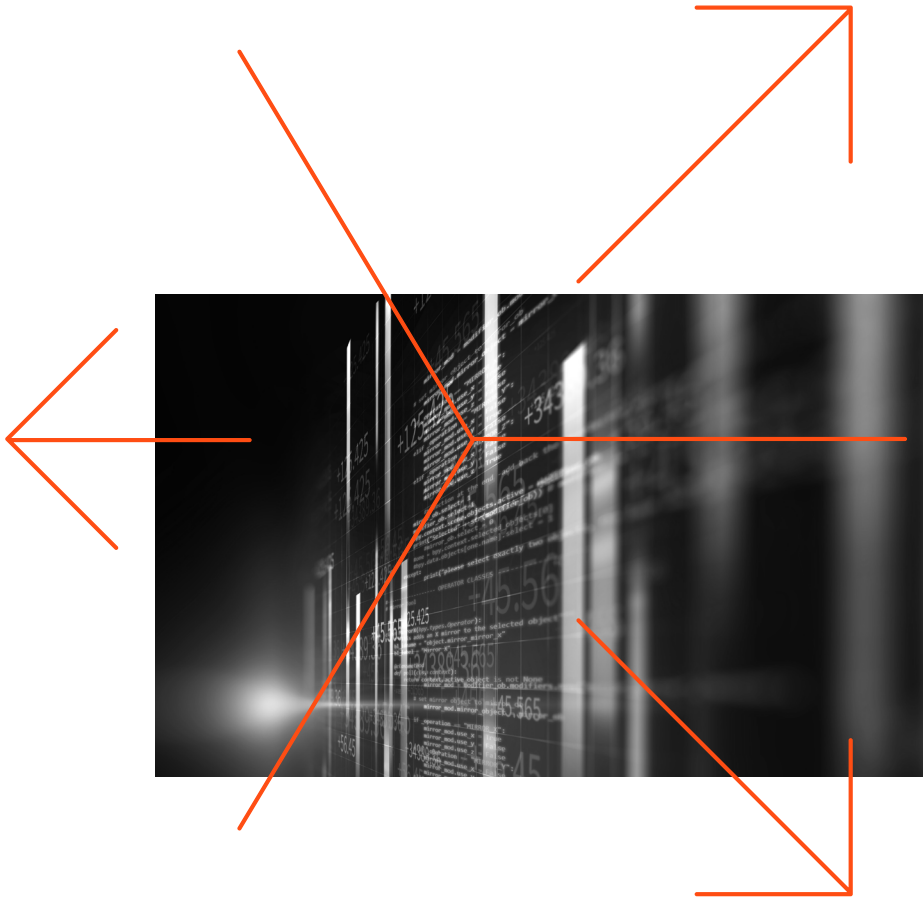
As the threat landscape evolves, is your organization ready to defend against advanced cyber attacks?

Without a robust, ongoing process for evaluating the effectiveness of your cybersecurity team, technology, policies and practices, it's difficult to have an adequate understanding of your cybersecurity readiness.

Periodic cyber risk assessments are necessary to:

- **Establish** a baseline for measuring cybersecurity progress or regression over time
- **Plan** for required training, process changes and network/software improvements
- **Generate** reports for cyber insurance qualification and service level agreement grading
- **Provide** evidence of due diligence to regulatory bodies in the event of a breach

Even if you already conduct cyber risk assessments, many available tools cannot fully emulate your network, infrastructure, software and processes, as well as typical and adversary traffic patterns and behavior. To stay ahead of threats, you need a powerful solution that simulates attack campaigns, scores detection and defense, tracks performance metrics and benchmarks results.



Gain unprecedented insight into the state of your cyber detection, defense and mitigation systems

Powered by the SimSpace Cyber Risk Management Platform, which includes the most realistic cyber range on the market, Cyber Risk Assessments allow you to evaluate your defenses against a backdrop of compliant and non-compliant user and administrator activities, automated threat behaviors and adversary campaigns.

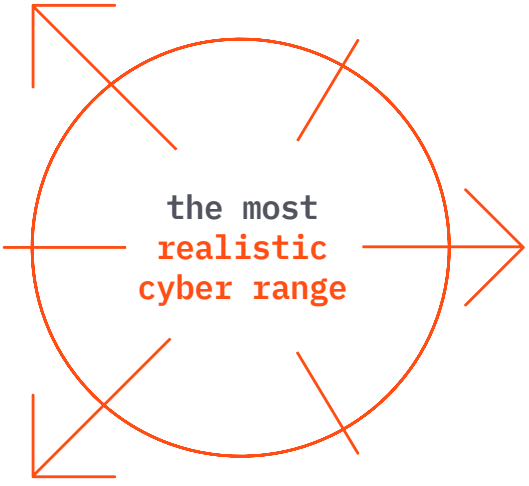
Suitable for both large enterprises and small organizations, this robust capability helps you assess and build teams, implement process changes, and make technology investments to improve your cybersecurity posture.

The solution accurately measures key performance indicators, including defensive success rate, time to detection, time to effective response and threat mitigation rate—with scores and analysis available within minutes of event completion. In addition, event reports allow you to benchmark performance and measure progress against industry-standard frameworks and anonymized peer data.

SimSpace provides unmatched flexibility to set up your cyber range as a SaaS platform, on-premises via a client network or as a network-attached appliance.

Who will benefit?

- Chief information security officers
- Executives and senior managers
- Cybersecurity teams
- IT teams
- Legal and compliance teams



flexible

Stress-test your defenses with a library of pre-built automated attacks

The SimSpace Platform uses our proprietary Cyber Range Attack for Training (CRAFT) framework to model sophisticated adversary behaviors like advanced persistent threats (APTs). CRAFT covers initial compromise, lateral movement around the network, targeting of specific assets, setup of command-and-control channels, data exfiltration and post-attack cleanup.

You can run automated attack scenarios for both legacy and emerging threat models, including adversaries such as APT3, APT10 and APT40, as well as common attack behaviors like beaconing, reconnaissance and exploitation of a domain controller. You can also customize attack scenarios to meet your organization's specific needs:

- Vulnerability regression testing
- Comparison of defense team performance
- Attack flexibility to challenge the most adept security teams and tools

CRAFT at a glance

- Uses a variety of real-world attacks and tools, such as the MITRE ATT&CK® Framework
- Provides the latest intelligence for modeling specific relevant threats
- Leverages the Wormhole zero-day emulator to gain access to a host and evade defensive tools
- Modifies attack behaviors during execution by varying the time between attack steps and forcing mistakes in the adversary workflow

Built-in intelligence

Attack scenarios use an AI-powered orchestrator to adjust actions, target systems and attack paths—alternating tools and techniques in response to network changes or defensive actions.

Randomization

The solution employs randomization throughout the attacks to target equivalent sets of machines, maximize reuse and allow teams to repeat attack scenarios.

Bypass capability

If an entry point is well protected, a simulated attack can vary its vectors to jump through that defense and continue to test other areas within the network. This provides a more thorough evaluation of your security team and technology stack.

Event historian

As automated attack scenarios run on your network, the status of each phase is posted to the Event Historian. Our scoring engines use this data to automatically assess team performance based on established objectives.

objective

Measure team performance with objective scoring

SimSpace Cyber Risk Assessments evaluate and track participant actions during the execution phase of any assessment event, such as a live red-team campaign involving multiple attack scenarios:

- Assess blue team performance based on their ability to defend against attacks
- Evaluate organizational processes during cyber range events and determine attack success rates
- Prepare reports for executive leadership to demonstrate program progress

Success or failure rating

Our objective scoring system assigns a success or failure rating for each attack scenario modeled. These scores will map to one result from a tiered system of expectations:

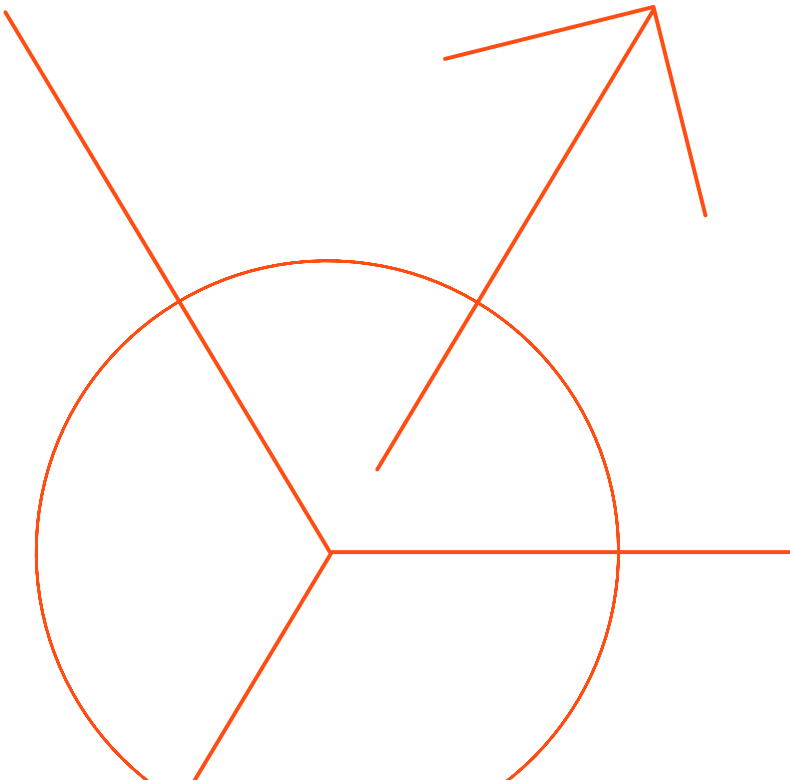
- Needs improvement (default score when an attack is successful)
- Below expectations
- Meets expectations
- Exceeds expectations
- Excluded from scoring

Bias control

You can eliminate bias in scoring by separating event manager and attack creator domains of responsibility. In addition, event assessors have the flexibility to exercise discretion while evaluating final scores.

Actionable insights

Event reports provide baseline assessment results and pinpoint areas of weakness to drive continuous improvement across people, processes and technology. You can use this data to inform plans aimed at optimizing your organization's overall cyber health.



Did you know?
Security personnel can earn CPE credits by completing training courses on our cyber range platform, or by attending SimSpace virtual events.

SimSpace Cyber Risk Management Platform features

- Open, customizable, high-fidelity platform
- Library of automated cyber crisis training content, APTs, insider threats and zero-day attacks
- Support for top open-source and commercial cybersecurity products
- Insights from our Professional Services team
- Pre-built, industry-specific network templates—hybrid cloud, ICS and SCADA
- Advanced user emulation for realism and more meaningful assessments
- Data-driven product evaluation and tech-stack tuning
- Maps to NICE 3.0, MITRE ATT&CK® and other regulatory frameworks

actionable

Learn more

Ready to learn more about how SimSpace Cyber Risk Assessments can help your organization build cyber readiness? Click here to request a demo.