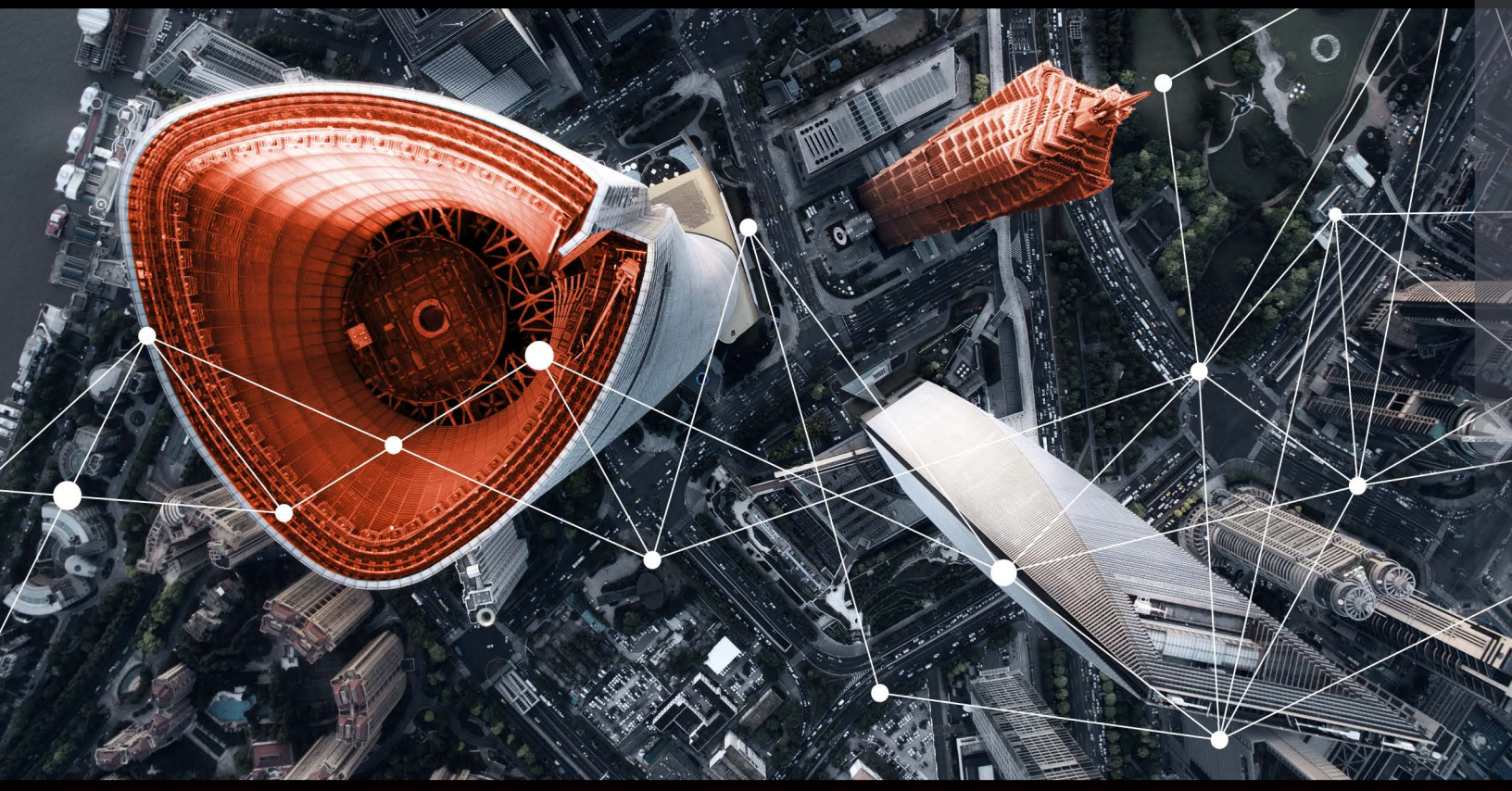
DATASHEET

SIMSPACE

CYBER RISK MANAGEMENT FOR TELECOMMUNICATIONS



KEEP SYSTEMS AND NETWORKS ONLINE

MANAGE GROWING IoT DEMANDS

REALIZE DIGITAL TRANSFORMATION

TELECOM

SIMSPACE
SECURE WITH CONFIDENCE

Today, telecommunications companies (telcos) support businesses, consumers and nation-states by providing the connectivity needed to drive everything from email and messaging to video conferencing, mobile communications and entire news outlets. Because telcos support information exchange for government and industry, they represent a critical component of our infrastructure and are a major target for threat actors–including insiders–seeking access to sensitive data or disrupting communications.

As companies roll out 5G networks and other digital transformation projects, the attack surface will only continue to expand—further escalating the risks to critical infrastructure, business continuity and customer data privacy associated with threat techniques like phishing, malware, APTs and DDoS attacks.

The criticality and sensitivity of the data handled, as well as the size of the customer base, make this a highly regulated sector. To keep pace with stringent compliance requirements, evolving threats and technological advancements like the Internet of Things (IoT), telcos need to have their security teams and tech stacks performing optimally, which requires continuous assessments under realistic conditions.

stay connected

With the SimSpace Cyber Risk Management Platform, you can use the most advanced commercially-available cyber range to stand up secure, high-fidelity simulations of your production environment for team training and technology optimization.

Secure connectivity and growth starts with cyber readiness

When your security teams and technology are able to effectively identify and mitigate cyber threats, you'll be more equipped to expand your offerings without risking breaches and service interruptions. Give your personnel the hands-on-keyboard experience they need to defend against advanced threats and optimize your security stack by seeing how your tools perform in a life-like production simulation.

Build team readiness with SimSpace

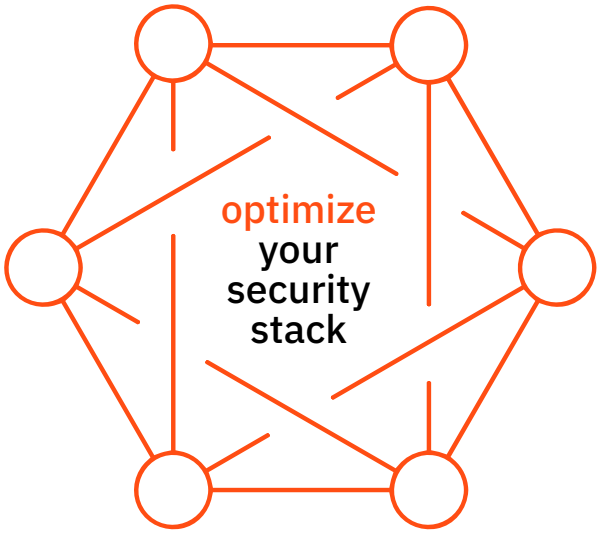
- Establish a baseline for your security posture
- Introduce new attacks and penetration testing scenarios to challenge and prepare your team
- Collect data and run analytics to measure team performance
- Run more scenarios to improve your security posture and team proficiency

54%

Percentage of the 500 largest DDoS attacks in Q4 2021 targeting telecom companies[1]

150,000

Average number of threats against the industry interrupted per week in 2021[2]



Maintain industry certifications

Our partnership with (ISC)² allows us to directly submit CPE activity. That means you and your team can earn credits by completing training courses on our cyber range or attending SimSpace virtual events.

[1] Lumen Quarterly DDoS Report. (2022). Lumen. https://pages.lumentech.com/DDoS-Threat-Report-LP.html

[2] Darktrace Reports Information Technology and Communications Sector Most Targeted by Cyber-Attackers in 2021 | Press Releases. (2021). Darktrace. https://www.darktrace.com/en/press/2021/387/

Evaluate your defenses under realistic conditions

With SimSpace, you can see how your personnel respond to advanced cyber threats with the same security tools they use on the job:

- Conduct live-fire exercises and pen tests
- Practice defending against APTs, DDoS attacks, insider threats and more
- Develop role-specific skills
- Validate your security policies and processes
- Map security assessments to regulatory standards such as NIST, CISA and the FCC CSRIC

Build security into your offerings without slowing delivery

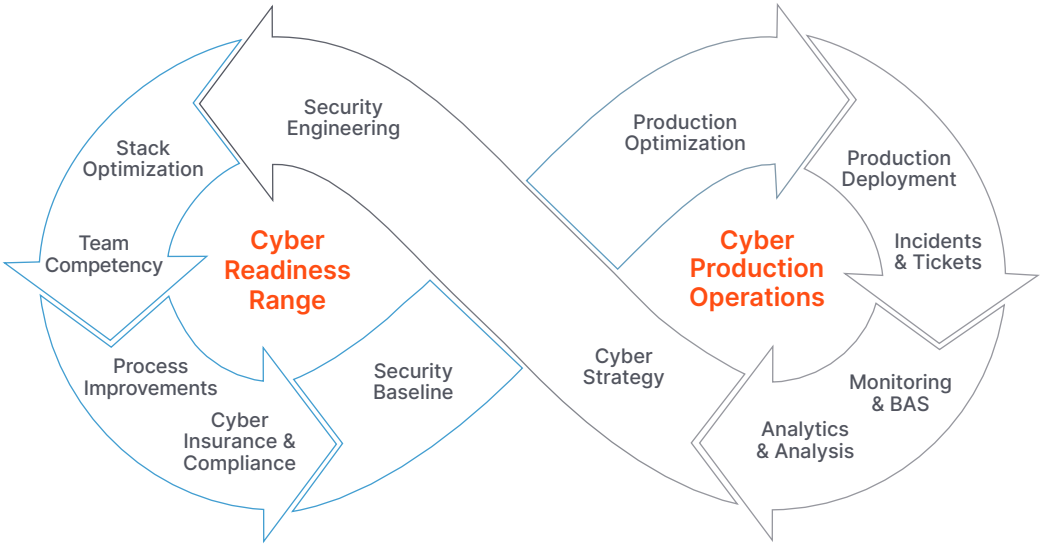
- Understand how security tools and policies impact business operations
- Develop more secure applications, configurations and operating models
- Test new patches and integrations
- Tune your tech stack using objective performance metrics
- Perform in-depth product evaluations before making a purchase

Business results

- Keep networks and communications systems online
- Safeguard customer data to build trust
- Demonstrate compliance for regulators and cyber insurance
- Optimize vendor selection
- Secure the growing IoT attack surface
- Enable new digital offerings and revenue streams

stay secure

Make informed decisions throughout the cyber-maturity lifecycle



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

Why SimSpace?

Our exclusive cyber range provides telcos with an unparalleled platform for cyber risk assessments, product evaluation, real-world attack simulations and extensive individual and team readiness training. SimSpace helps you up-level your security posture and team competency, so you can defend against evolving cyber threats with confidence. As a result, you'll be able to meet operational goals, protect your brand value and stay compliant.

World's most realistic cyber range

Trusted by 5 of the Top 10 US banks

Chosen by the US Cyber Command

40% reduction in configuration related breaches

45% improvement in attack defense

48% improvement in time to detect attacks

Click here to learn more about how SimSpace can help you assess and optimize the performance of your security team and tech stack.

simspace.com info@simspace.com

SIMSPACE