DATA SHEET

SIMSPACE
SECURE WITH CONFIDENCE

Continuous Security Improvement for

Global Cyber Defense Organizations

Government, military, and intelligence agencies, as well as national critical infrastructure, are often targeted by cybercriminals and nation-state threat actors seeking access to sensitive data for financial or geopolitical gain. As sophisticated attacks in the form of malware, APTs, and social engineering continue to be launched against government networks and infrastructure across the globe, any entity handling data or controls that impact national security or other necessities needs to ensure that its personnel, processes, and security tools can defend against advanced threats.

The SimSpace Cyber Force Platform, the same solution used by the US Cyber Command, allows military and government agencies to train for real-world cyber-crisis scenarios within a realistic simulation of their networks, including IoT, ICS, SCADA, OT, CNI, cloud, and hybrid-cloud systems. With its high-fidelity, military-grade cyber range, SimSpace provides a safe, isolated, and realistic environment to train against advanced cyberattacks using the same security tools your cyber defense teams already use on the job.

The SimSpace Cyber Force Platform allows military and government agencies to train for real-world cyber-crisis scenarios within a realistic simulation of their networks.

Train the same way you fight

The SimSpace Cyber Force Platform provides an unparalleled solution for security assessments, product evaluation, real-world attack simulations, and extensive individual and team readiness training. In addition, SimSpace offers advanced tools and services to help organizations make smarter decisions around risk, compliance, and security deployments.

- Elite special-forces training for cyber ops and nation-state defenders
- High-fidelity cyber range replicates your full IT infrastructure, including on-prem, cloud, and physical systems
- Flexible platform supports mission rehearsals, Live-Fire Experiences (LFXs), and team certifications
- Realistic threats, such as APTs, malicious insiders, and zero-day exploits help expose gaps in team readiness and technology performance
- User Emulation technology simulates routine network traffic and background noise to help cyber defenders differentiate between normal and malicious activity

Drive continuous security improvement

Keeping pace with a dynamic threat environment requires ongoing assessments and training events. SimSpace helps build stronger team dynamics over time with scalable, repeatable exercises and elite-level training content:

- Establish your baseline security performance
- Introduce cyberattacks and pen testing scenarios to challenge your teams
- Leverage objective performance data and analytics on team and technology performance
- Run more training scenarios to further improve your security posture and team proficiency

Optimize your security stack

Seeing how your security stack functions in a digital twin of your IT infrastructure allows you to optimize configurations before pushing to production. You can even evaluate the impact of adding a new security tool, so you can make more informed technology decisions.

- Conduct data-driven assessments of security products with the help of our expert Professional Services team
- Map technology assessments to the MITRE procedures map, which provides a deeper understanding of your tech stack's coverage, strengths, and weaknesses
- Access objective performance metrics to understand the security and operational impact of a new piece of technology

Key results

Keeping pace with a dynamic threat environment requires ongoing assessments and training events. SimSpace helps build stronger team dynamics over time with scalable, repeatable exercises and elite-level training content:

- **Comprehensive compliance documentation** - Verify that your security controls and configurations are consistent with regulatory requirements
- **Increased network uptime** - Keep critical systems, networks, and national infrastructure online by building your cyber defense capabilities
- **Stronger team dynamics** - Build out seamless processes and orchestrate more efficient handoffs through live-fire team-training events
- **Improved data security** - Safeguard sensitive information that can impact national security by teaching your security teams to defend against advanced nation-state threats
- **Reduced supply-chain risk** - Understand the security impact of onboarding a new service without jeopardizing the security of your systems and networks

Ready to learn more about how SimSpace's battle-tested solutions can help government, military, and intelligence agencies protect critical systems, data, and infrastructure? Visit simspace.com to request a demo.