DATA SHEET

SIMSPACE
SECURE WITH CONFIDENCE

SimSpace Cyber Force Platform for Critical Infrastructure

The acceleration of digital technology improvements in the critical infrastructure sector has greatly increased the performance and efficiency of these systems. However, these improvements also have a downside, as they contribute to greater cyber exposure. And the prominence of critical infrastructures, such as telecommunications, makes these industries a significant target for cyber attackers. Cyberattacks on critical infrastructure can be physically and financially detrimental, leading to safety issues, unscheduled downtime, and reputational impact.

Key benefits

- Protect the most vulnerable and strategic assets
- Increase the visibility of operational technology (OT) assets
- Prepare to defend against emerging threats
- Develop an understanding of how OT and IT assets converge
- Coordinate between the public and private sectors

In the face of uncertainty, such as ransomware attacks, global pandemics, supply chain disruptions, and increasing geopolitical unrest, public and private organizations are evaluating their operational cyber readiness, including protection of operational technology (OT).

The SimSpace Cyber Force platform helps CISOs and their teams shield their most vulnerable and strategic OT and IT assets from devastating cyberattacks by driving continuous improvements in their security programs. With our military-grade cyber range, teams can model their digital infrastructure to understand how an emerging cyber threat would affect their entire environment. That’s why government and private organizations trust SimSpace to help them better defend their critical infrastructure.

Deploy battle-tested, guaranteed-safe cyber simulations to validate your people, processes, and technology

People

- Coordinate between public and private entities
- Train personnel on possible threats to IT and OT environments

Processes

- Understand the state of your cybersecurity program
- Improve information-sharing processes to protect critical infrastructure from cyberattacks
- Incorporate emerging security directives for critical infrastructure into your governance strategy

Technology

- Assess your defenses against emerging threats
- Duplicate your entire environment, including OT and IT assets for training and evaluations
- Coordinate security management for OT, IoT, IIoT, and IT devices

Gain visibility of all assets in your environment

Organizations cannot effectively protect assets they don't know about. To properly understand your entire attack surface, it's critical to have visibility into all assets on your network, including critical infrastructure assets. Training on a cyber range can help cybersecurity operators learn to gain insight into those assets.

Business results

- Protect critical processes to avoid lethal consequences
- Understand the increased speed and complexity of emerging threats to prepare and modernize critical infrastructure security
- Improve management and security across IT and OT systems

Gartner expects that by 2025, 70% of asset-intensive organizations will merge their security functions across enterprise and operational environments.

External connections to OT devices more than doubled in 2021, with 70% of organizations running OT assets that can be accessed remotely. - Dragos 2021 Year in Review

Only 18% of companies restrict network access and enforce MFA to access OT networks remotely. - The State of Industrial Security in 2022, Barracuda Networks

Only 45% of organizations think they are effective in discovering and maintaining an inventory of all devices attached to the OT network. - Ponemon Institute

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

SimSpace Cyber Force Platform features

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

Why SimSpace?

The SimSpace Cyber Force Platform is powered by our military-grade cyber range that provides critical infrastructure — including energy, telecom, and manufacturing — with an unparalleled platform to validate security stack effectiveness, test people, processes, and technology, and identify cost reduction opportunities in a guaranteed-safe simulation environment. SimSpace helps you uplevel your security posture and team competency to defend against evolving cyber threats with confidence. As a result, you'll be able to improve operational efficiency, protect your brand value, and incorporate security directives into your governance strategy.

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

Every effort has been made to ensure the information contained herein is accurate and up-to-date but is provided "as is" with no representations or warranties of any kind, express or implied, with respect to the information provided or any subsequent changes to the information provided. This edition supersedes all previous collateral.