



## Company Overview

SimSpace Corporation launched in 2015 with a singular purpose — to help public and private entities develop their cybersecurity teams, protect strategic assets, and manage risk.

Built by experts from the U.S. Cyber Command and the NSA, the SimSpace Cyber Force Platform leverages technology developed at MIT Lincoln Laboratory to address the toughest cybersecurity questions facing CISOs and other security professionals.

Our military-grade cyber ranges are used by the U.S. military, the global intelligence community, critical infrastructure, and top financial institutions to generate high-fidelity simulated environments. Through ongoing training events and powerful analytics, these simulations provide quantitative insights that help drive continuous improvements across people, processes, and technology.



The SimSpace Cyber Force Platform provides the only battle-tested cyber range on the market, so you can evaluate your defenses under realistic conditions.

• **Open cyber range platform** - Stand up high-fidelity simulations of IT environments that include on-prem, cloud, remote edge, OT, IOT, ICS, OTC, and SCADA systems.

• **Attack simulations** - Automatically recreate nation-state level attacks like zero-days, APTs, malicious insiders, and other real-world incidents without impacting production.

• **Actionable insights** - Access performance metrics for data-driven insights into security program maturity, team readiness, and organizational cyber risk.

• **Swift range set-up and scale** - SimSpace Rapid Range™ automates, scales, and validates the replica of your production environment, reducing cyber range deployment times from days to hours.

• **Cyber evidence** - Customers can source cyber evidence from live-fire exercises, allowing them to use the insights for auditor requirements, regulatory reports, and workforce management and demonstrate improvements for cyberinsurance providers.

• **Build custom exercises** - Manage attacks and build campaign-specific live-fire exercises. Provide detailed information about each attack scenario and outcome to meet your security validation requirements.

## Company Overview

Thank you for downloading this SimSpace data sheet! Carahsoft is the distributor for SimSpace cybersecurity solutions available via NASA SEWP V and other contract vehicles.

To learn how to take the next step toward acquiring SimSpace's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/SimSpaceResources](https://carah.io/SimSpaceResources)



For upcoming events:  
[carah.io/SimSpaceEvents](https://carah.io/SimSpaceEvents)



For additional SimSpace solutions:  
[carah.io/SimSpaceSolutions](https://carah.io/SimSpaceSolutions)



For additional cybersecurity solutions:  
[carah.io/Cybersecurity](https://carah.io/Cybersecurity)



To set up a meeting:  
[SimSpace@carahsoft.com](mailto:SimSpace@carahsoft.com)  
844-445-5688



To purchase, check out the contract vehicles available for procurement:  
[carah.io/SimSpaceContracts](https://carah.io/SimSpaceContracts)

# Company Overview

SimSpace Corporation launched in 2015 with a singular purpose – to help public and private entities develop their cybersecurity teams, protect strategic assets, and manage risk.

Built by experts from the U.S. Cyber Command and the NSA, the SimSpace Cyber Force Platform leverages technology developed at MIT Lincoln Laboratory to address the toughest cybersecurity questions facing CISOs and other security professionals.

Our military-grade cyber ranges are used by the U.S. military, the global intelligence community, critical infrastructure, and top financial institutions to generate high-fidelity simulated environments. Through ongoing training events and powerful analytics, these simulations provide quantitative insights that help drive continuous improvements across people, processes, and technology.

The SimSpace Cyber Force Platform provides the only battle-tested cyber range on the market, so you can evaluate your defenses under realistic conditions.

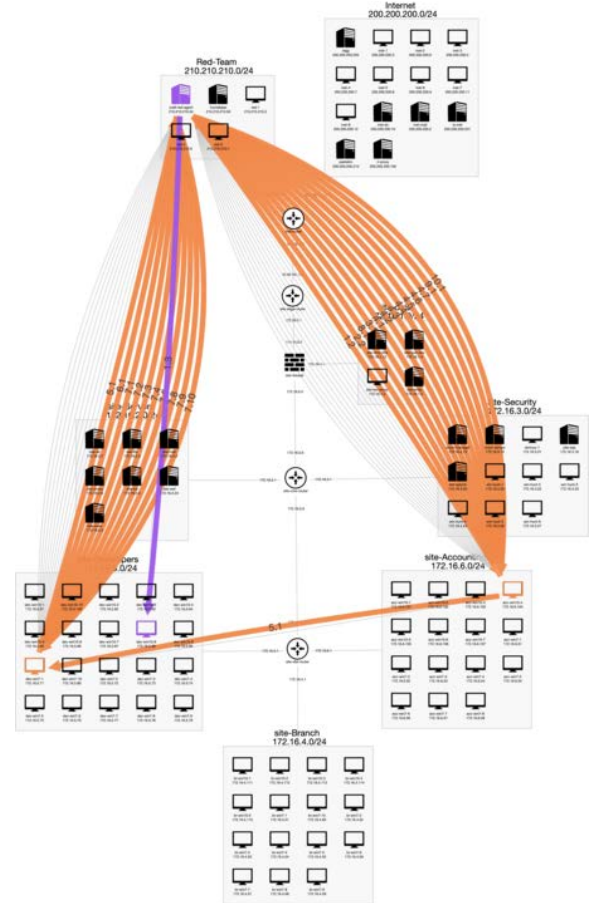
- ▶ **Open cyber range platform** - Stand up high-fidelity simulations of IT environments that include on-prem, cloud, remote, edge, OT, IoT, ICS, CNI, and SCADA systems
- ▶ **Attack simulations** - Automatically recreate nation-state-level attacks like zero-days, APTs, malicious insiders, and other real-world incidents without impacting production
- ▶ **Actionable insights** - Access performance metrics for data-driven insights into security program maturity, team readiness, and organizational cyber risk
- ▶ **Swift range set-up and scale** - SimSpace Rapid Range<sup>SM</sup> automates, scales, and validates the replica of your production environment, reducing cyber range deployment times from days to hours
- ▶ **Cyber evidence** - Customers can source cyber evidence from live-fire exercises, allowing them to use the insights for auditor requirements, regulatory reports, and workforce management and demonstrate improvements for cyberinsurance providers
- ▶ **Build custom exercises** - Manage attacks and build campaign-specific live-fire exercises. Provide detailed information about each attack scenario and outcome to meet your security validation requirements.



## The SimSpace advantage

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.

- Guaranteed-safe, sophisticated simulation environments to test and validate your people, processes, and technology
- Provide detailed analytics to inform boards and executives and to meet requirements for regulators and insurers.
- Dynamic, hands-on skills development to enable elite cyber professionals
- Security assessments map to NICE 3.0, MITRE ATT&CK®, and other regulatory frameworks
- Intelligent, host-based user emulation creates a realistic training setting complete with network traffic
- Library of elite special forces-level training content, APTs, insider threats, and zero-day attacks
- Quantitative metrics validate security stack effectiveness, drive operational efficiency, and identify cost reduction opportunities



*Threat actions tracked within the cyber range*

### Did you know?

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

Ready to learn more about how SimSpace can deliver intelligence-community validated techniques and processes for continuous security improvements? Click [here](#) to request a demo.