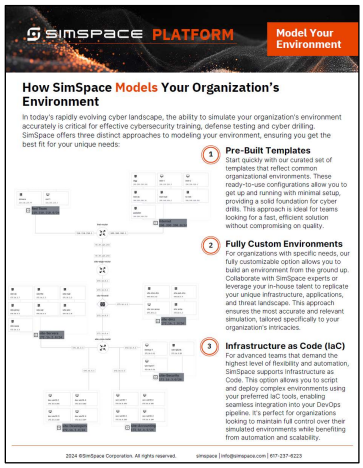


How SimSpace Models Your Organization's Environment

Thank you for downloading this SimSpace resource. Carahsoft is the distributor for SimSpace Cybersecurity solutions available via NASA SEWP V, ITES-SW2, NASPO ValuePoint, 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

For upcoming events:
carah.io/SimSpaceEvents

For additional Bastille solutions:
carah.io/SimSpaceSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
SimSpace@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/SimSpaceContracts

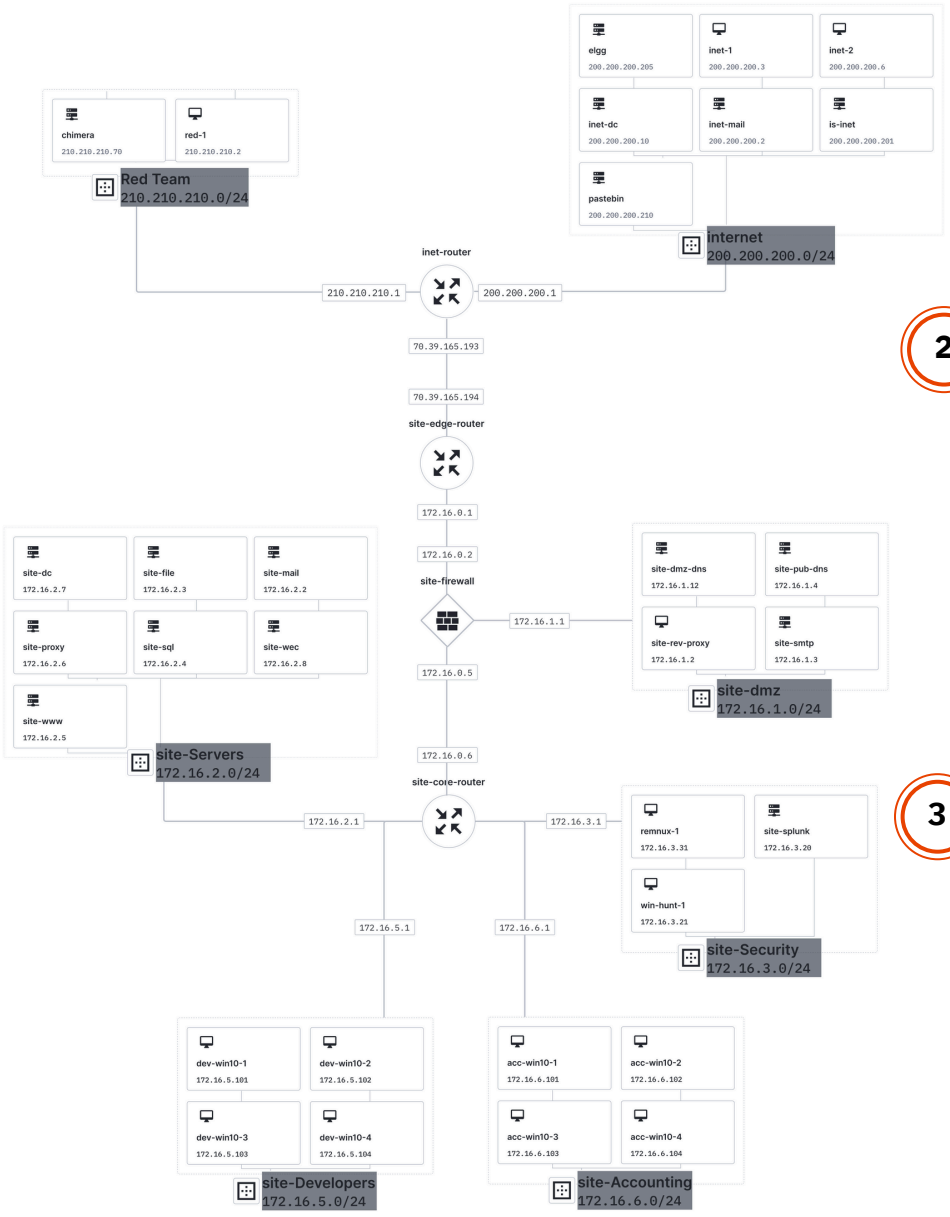
For more information, contact Carahsoft or our reseller partners:
SimSpace@carahsoft.com | 844-445-5688

SIMSPACE PLATFORM

Model Your Environment

How SimSpace Models Your Organization's Environment

In today's rapidly evolving cyber landscape, the ability to simulate your organization's environment accurately is critical for effective cybersecurity training, defense testing and cyber drilling. SimSpace offers three distinct approaches to modeling your environment, ensuring you get the best fit for your unique needs:



1 Pre-Built Templates

Start quickly with our curated set of templates that reflect common organizational environments. These ready-to-use configurations allow you to get up and running with minimal setup, providing a solid foundation for cyber drills. This approach is ideal for teams looking for a fast, efficient solution without compromising on quality.

2 Fully Custom Environments

For organizations with specific needs, our fully customizable option allows you to build an environment from the ground up. Collaborate with SimSpace experts or leverage your in-house talent to replicate your unique infrastructure, applications, and threat landscape. This approach ensures the most accurate and relevant simulation, tailored specifically to your organization's intricacies.

3 Infrastructure as Code (IaC)

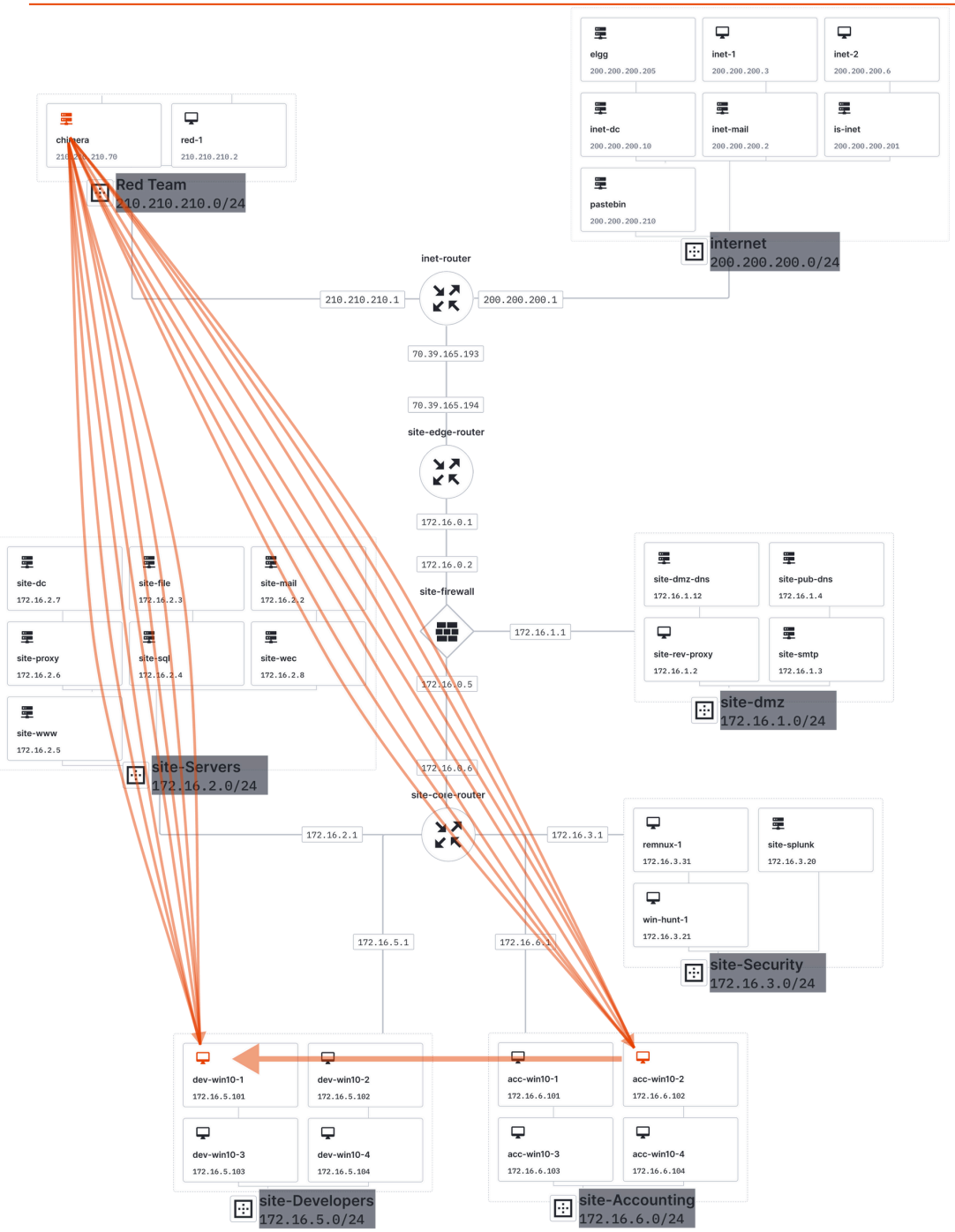
For advanced teams that demand the highest level of flexibility and automation, SimSpace supports Infrastructure as Code. This option allows you to script and deploy complex environments using your preferred IaC tools, enabling seamless integration into your DevOps pipeline. It's perfect for organizations looking to maintain full control over their simulated environments while benefiting from automation and scalability.

SIMSPACE PLATFORM

Model Your Environment

Emulate Real Threats in Your Modeled Environment

Once your environment is accurately modeled within SimSpace, the next step is to test its resilience against real-world threats. SimSpace's advanced threat emulation capabilities empower you to go beyond traditional security testing, offering unparalleled insight into your organization's true defensive capabilities.



Based on Real Threat Actors

We use the latest industry intelligence to emulate how real threat actors operate, creating attack scenarios that mirror actual tactics, techniques, and procedures.

Real Attacks

Unlike BAS tools or automated penetration testing that often use defanged or simplified attacks, SimSpace runs full, realistic attacks, including authentic payloads, procedures, and lateral movements.

Atomic Testing

Our granular approach allows for realistic team drills, unlocking the ability to test your security team's efficacy in handling true-to-life threat scenarios.

Request an Expert-Led Call

During this call we will cover:

- How we enable your ability to create a digital twin
- Use cases specific to your organization's needs

simspace | info@simspace.com | 617-237-6223