

SimSpace - CTEM Data Sheet

Thank you for downloading this SimSpace datasheet. 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

In today's rapidly evolving threat landscape, the ability to continuously **assess, improve** and **validate** your organization's cybersecurity posture is critical. SimSpace's tailored cyber range provides the ideal environment to enhance your Continuous Threat Exposure Management (CTEM) strategy, allowing your team to anticipate, identify, and mitigate threats with precision and assurance.

What is CTEM?

Continuous Threat Exposure Management (CTEM) is a comprehensive framework designed to optimize exposure risk reduction within a security program. It involves the continuous process of identifying, measuring, and mitigating cyber threats, ensuring that your organization remains resilient against ever-evolving challenges.

SimSpace Enhances CTEM



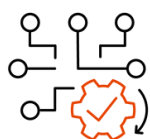
Enhanced Threat Identification

SimSpace provides realistic threat emulations, enabling teams to identify a wide array of threats and vulnerabilities within an organization, **reducing their mean time to detect** threats in the future.



Exposure Identification

SimSpace uncovers and helps map potential exposure points in tools and processes, ensuring no vulnerabilities are overlooked and **reducing vulnerability density** for an organization.



Continuous Testing and Validation

SimSpace facilitates continuous testing of your security controls, helping you uncover and map exposure points while validating control effectiveness, ultimately **increasing the vulnerability detection rate** of an organization.



Implementation Assurance

SimSpace supports the implementation of mitigation strategies by emulating real-world scenarios, allowing organizations to test mitigation efforts before production, ensuring an effective execution and ultimately **reducing the mean time to respond** to threats in the future.

Core Components to CTEM

Continuous Threat Exposure Management (CTEM) allows organizations to identify, assess, mitigate and validate cyber threats and exposures in a continuous fashion. The SimSpace Platform is purpose-built to elevate all of the core elements of your CTEM strategy. By providing a realistic, tailored environment, our platform allows for enhanced threat and exposure identification, risk assessment, continuous testing and validation and implementation assurance.

1

Scoping

Identifying the scope of potential threats and vulnerabilities within an organization.

2

Discovery

Uncovering and mapping out all potential exposure points.

3

Prioritization

Assessing and ranking threats based on their potential impact and likelihood.

4

Validation

Testing and measuring the effectiveness of security controls and responses.

5

Mobilization

Implementing and executing mitigation strategies.

Why Choose SimSpace?

SimSpace's tailored cyber range goes beyond traditional testing environments. It offers a safe, controlled space to explore "what if" scenarios, enabling your team to identify gaps in existing controls without risking real-world business operations. With SimSpace, you can confidently enhance your CTEM framework and strengthen your organization's cybersecurity resilience.

Ready to take your CTEM strategy to the next level? Contact SimSpace to schedule a demo and see how our cyber range can transform your security posture.

Request an Expert-Led CTEM Strategy Call



During this call we will cover:

- Our CTEM lead approach
- How we enhance your threat management capabilities
- Use cases specific to your organization's needs