



SimSpace Corporation

Battle-Ready Cybersecurity as a Testbed

SimSpace Overview – Battle-Ready Cybersecurity as a Testbed

- The Cyber Force Platform used by [US Cyber Command*](#)
- CEO - William Hutchison, Senior Officer from the US Cyber Command
- CTO – Lee Rossey, Head of Cyber Security from MIT Lincoln Laboratory
- SIFMA “Quantum Dawn” Live-Fire Exercises
- Project Testbeds
 - **IARPA ReSCIND**
 - DARPA RADICS
- The SimSpace Cyber Force Platform delivers:
 - **Military-Grade Cyber Ranges**
 - **Elite Force Training**
 - **Live-Fire Exercises**





SIMSPACE

BATTLE-READY CYBERSECURITY



The SimSpace Cyber Force Platform (CFP) is the **primary cyber range** of the US Cyber Command



#1 military cyber range provider capable of supporting complex, 25,000 live concurrent emulations



Cyber range provider to CI Sectors: **4 of the top 5 Global Banks** simulating 400,000 end-point environments



Cyber range provider to the **"Five Eyes" & intelligence community**



Highest fidelity environments sophisticated use cases with an organization's own defensive tools

What Are the Capabilities of the Cyber Force Platform?

Military-Grade Cyber Range

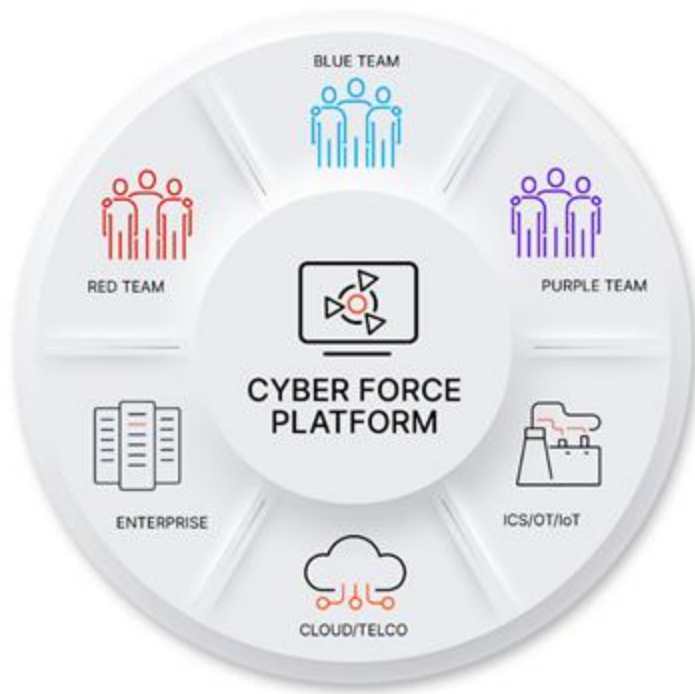
Provides high-fidelity replications of any cyber environment, including on-prem, clouds, remote/edge, OT, IoT, and ICS.

Live-Fire Exercises

Comprehensive live-fire exercises to test your cyber teams via Red/Blue/Purple exercises and CTF events.

Evaluate Cyber Warfare Platforms

Determine the efficacy and interconnectivity of weapons platforms within the Cyber domain in large-scale operations and assessments.



Guaranteed-Safe Simulation Environments

Simulate any cyber security environment on our cyber range to run live-fire exercises with no risk to production deployments.

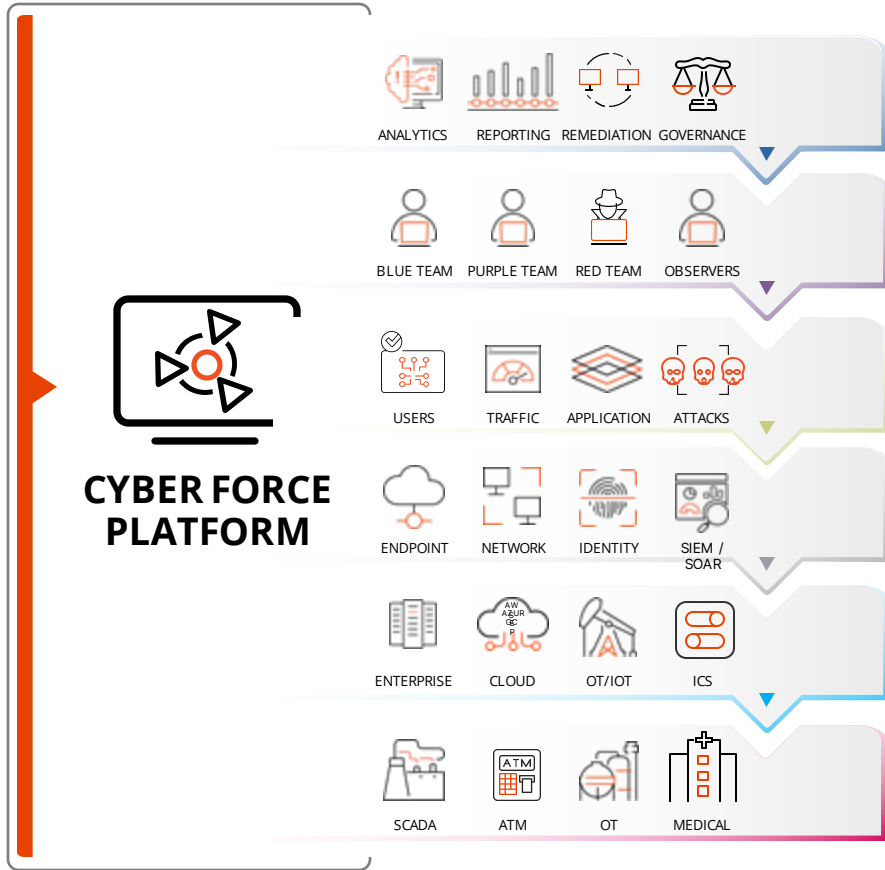
Advanced User and Attack Emulations

SimSpace provides the most advanced user emulations to create hyper-realistic attack event environments

Continuous Security Improvements

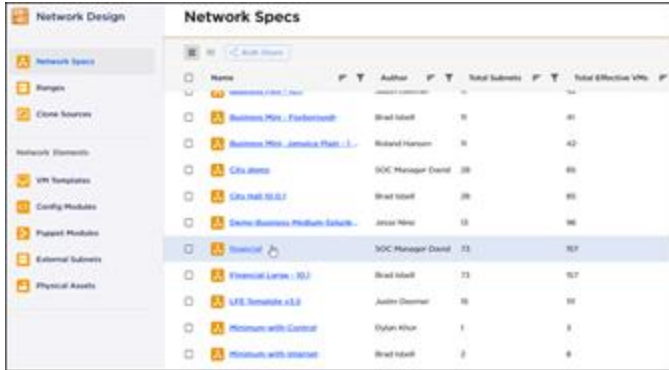
Benchmark your security posture and develop a measurable program to improve people, processes, and technology.

What is a Modern Cyber Range?



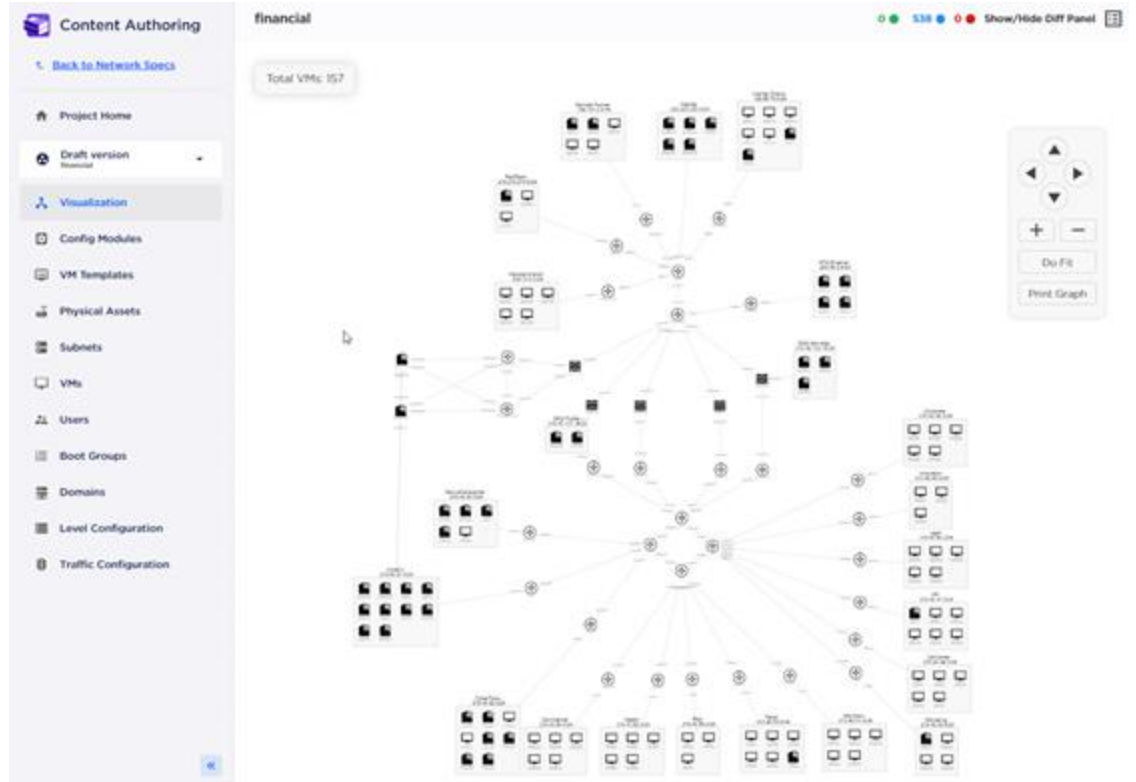
- 1 Connect Physical infrastructure**
Easily connect physical infrastructure that are critical to your global operations, including SCADA, ATM networks, cloud deployed IT, and other technology resources.
- 2 High-Fidelity, Guaranteed-Safe Replicas of Environments**
Validate every part of the IT terrain across your enterprise, examine process changes, & safely anticipate dynamic operational challenges and issues.
- 3 Replicate your Cyber Security Stack**
Answer the hard questions you cannot answer in your production environment, and follow up with a full suite of individual and team training and forensic capabilities where needed.
- 4 Real-World User Emulations and Attack Scenarios**
Test your team's performance against the most dangerous, real-world scenarios and drive areas for continuous improvement across your whole global infrastructure.
- 5 Elite Cyber Training and Live-Fire Events**
Train like you are going to fight against advanced adversaries in highly accurate replicas of your IT/OT environment, with your team, your processes and your tools.
- 6 Advanced Analytics and Reporting**
Get data-driven evidence about cyber readiness under adversity, exposures, cost reduction outcomes and provide operational transparency to senior leadership

Set Up Military Grade Ranges Quickly From Network Templates




Network Design Network Specs

Name	Author	Total Subnets	Total Effective VMs
Business Min - Facebook	Brad Isbell	31	41
Business Min - Jamaica Plain	Richard Hanson	31	42
CXs 2020	SOC Manager David	38	85
CXs 2021 01.01	Brad Isbell	38	85
Secur-Business-Platform-Security	Jason Nino	18	96
Technical	SOC Manager David	73	157
Financial Lanes - 01.1	Brad Isbell	73	157
LFE, Security v1.0	Justin Dorman	16	31
Minimum with Control	Elyan Khur	1	3
Minimum with Internet	Brad Isbell	2	6



Design custom ranges by hand or leverage network blueprint templates to quickly build and customize ranges

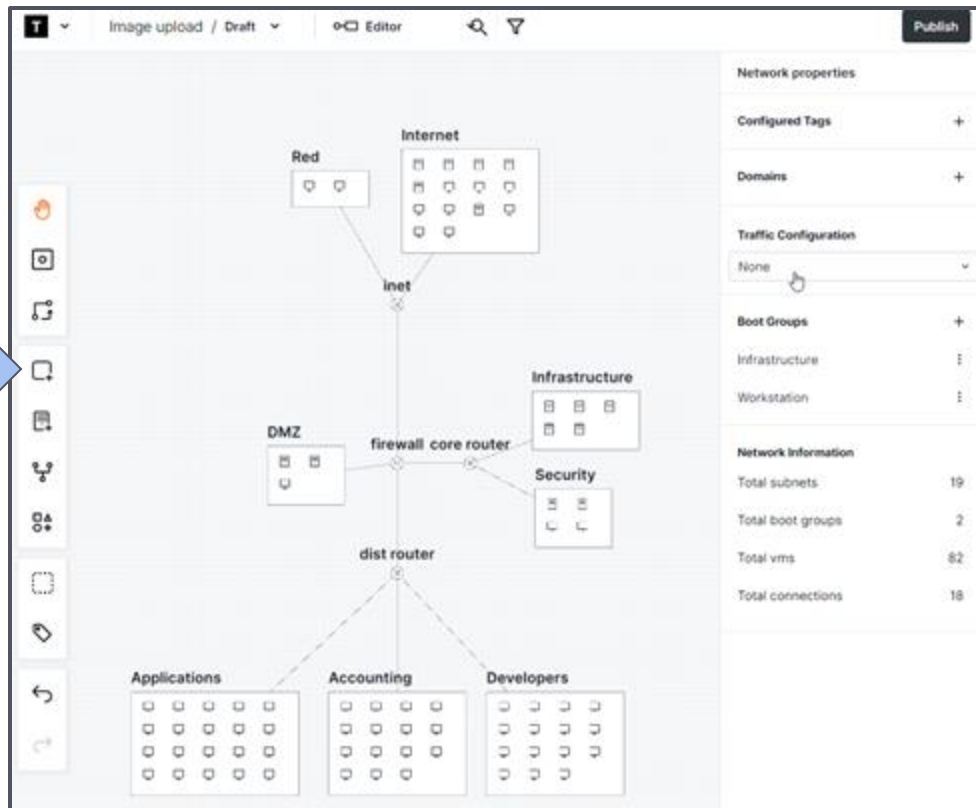
...or from Existing Production Data Sources

 **IT and security tool ingest** BETA

Use data from your production network as a starting point for your network.

Which security tools would you like to configure?

<input checked="" type="checkbox"/> Solarwinds BETA	<input checked="" type="checkbox"/> Addigy BETA
<input checked="" type="checkbox"/> CrowdStrike	<input checked="" type="checkbox"/> Rapid7 BETA
<input type="checkbox"/> Acunetix COMING SOON	<input type="checkbox"/> Cyber Reason COMING SOON
<input checked="" type="checkbox"/> Nessus BETA	<input type="checkbox"/> Ninja RMM COMING SOON
<input type="checkbox"/> Rumble COMING SOON	<input checked="" type="checkbox"/> GCP BETA



Perform Live Fire Team/Tech Training and Assessments

Library of Attack Scenarios

The screenshot displays the SimSpace Demo interface. On the left, there is a sidebar with 'Threat Actions' and a list of scenarios including 'Data Exfiltration from Shared Drive (APT40_1)'. The main area shows details for the selected scenario, including a 'Start' button, a description of the script's purpose, and a list of procedures and tactics. The status is 'Not Started' with a 'HIGH' severity level.

Threat Actions

Select a scenario from the Attack Campaign below to view details, control execution, or add notes.

Scheduled

Nothing Here

Add some scenarios to this Attack Campaign's schedule.

Not Scheduled

- Reconnaissance by an Insider Threat
- Data Exfiltration from Shared Drive (APT40_1)
- APT 40 Inspired Scenario 1
- Chimera Inspired scenario 1
- Domain Controller Service Disruption and Exfil
- Data Exfiltration via Phish Attack (APT10_1)
- Reconner Employment Scenario

Data Exfiltration from Shared Drive (APT40_1)

Start

This script implements one series of commands typically used by the threat actor commonly described as APT40. It infiltrates via a phishing attachment, moves laterally via a RemoteXy Scheduled Task, and exfiltrates data from that lateral host via a shared drive. Initial access takes one (1) second. Total approximate runtime: 6 minutes.

Not Started

Severity: HIGH

CRAPIT

Procedures

- PhishAttackMultiStage
- MimikatzDumpCreds

Uploads mimikatz and dump credentials. Returns the locked query for the hash for an input user.

Tactic and Techniques

Credential Access

Credential Dumping

HashCrack

Extracts credentials that have been stored as hashed values.

Tactic and Techniques

Credential Access

Brute Force

NetView

LogonScript

RemoteScheduledTask

Exercise Visualizations

The screenshot displays the SimSpace Demo interface showing network impact visualizations. The left sidebar lists a checklist of tasks for 'APT10_1', all of which are marked as completed. The main area shows a network diagram with nodes representing hosts and connections representing network activity.

Network Impact

View network activity involved in the execution of the Attack Campaign below.

APT10_1

- 1. PhishAttachment ✓
- 2. SimpleShellCLI ✓
- 3. IngressToolTransfer ✓
- 4. MimikatzDumpCr... ✓
- 5. RemoteSystems ✓
- 6. IngressToolTransfer ✓
- 7. IngressToolTransfer ✓
- 8. MimikatzPassThe... ✓
- 9. PersistTask ✓
- 10. ExfilOverC2 ✓

The network diagram shows a central node labeled 'Phish-Tool' connected to several other nodes, including '10.10.10.10', '10.10.10.11', and '10.10.10.12'. The connections are highlighted in orange, indicating active network activity.

SimSpace Contact Information

- Lee Rossey
- Co-Founder, CTO and Executive Sponsor
- e: lee@simspace.com

- Noam Ben-Asher
- Sr. Manager Attack Content & Product Incubation
- e: noam.ben.asher@simspace.com

- Jim Legg
- Director, Federal Programs
- e: jim.legg@simspace.com

Contact our team!

proposals@simspace.com

The logo consists of a stylized white 'S' shape with a small circle in the center, followed by the word 'SIMSPACE' in a bold, white, sans-serif font.

SIMSPACE