Capabilities Overview

SimSpace

The SimSpace Cyber Force Platform

SIMSPACE CYBER FORCE PLATFORM

Contents

Executive Summary

Introduction

SimSpace is the global leader in military-grade cyber ranges, founded by experts from U.S. Cyber Command and MIT's Lincoln Laboratory.

The company's Cyber Force Platform supports the most sophisticated enterprises, governments, and critical national infrastructure organizations.

SimSpace helps organizations continually improve their cybersecurity preparedness by providing high-fidelity simulation environments (virtualized, scaled down production replicas or digital twins), engaging training, and guaranteed safe, "live-fire" team training exercises.

SimSpace Corporation is an industry leader in conducting military-grade cyber-warfare simulations and is the trusted cybersecurity training provider of U.S. and foreign military services, the global intelligence community, and top private-sector organizations.

SimSpace's state-of-the-art network emulation and modeling tools provide high-fidelity, quantitative insights into how an organization can protect its critical assets against "lethal" cyber threats.

SimSpace has a long history of developing continuous security improvement solutions and supporting nation-state level exercises using our advanced range based capabilities.

Accomplishments since its founding in 2015 include:

- Primary vendor for the U.S. DoD's Persistent Cyber Training Environment (PCTE); which supports over 6,000 Cyber Mission Force members of the U.S. CYBER COMMAND. It is one of the world's largest and most complex Cyber Range Environments with over seven regional data centers and an aggregate capacity of over 50,000 virtual machines.
- 5 of the top 10 U.S. financial institutions rely on SimSpace.
- Selected as the Cyber Range for a Wall Street industry wide resilience exercise: SIFMA's Quantum Dawn in 2017.
- Led NYC Exercise for Critical Infrastructure (with Army Cyber Institute & Citi) in August 2016.
- Selected by DHS to provide simulated environments for cybersecurity product testing for U.S. critical infrastructure.
- Selected by DARPA to develop testbeds to assess innovative technologies for detecting and responding to cyberattacks on the U.S. electrical grid.
- The 5 Eyes intelligence community, as well as numerous government MoDs and intelligence agencies across APJ and EMEA have deployed SimSpace

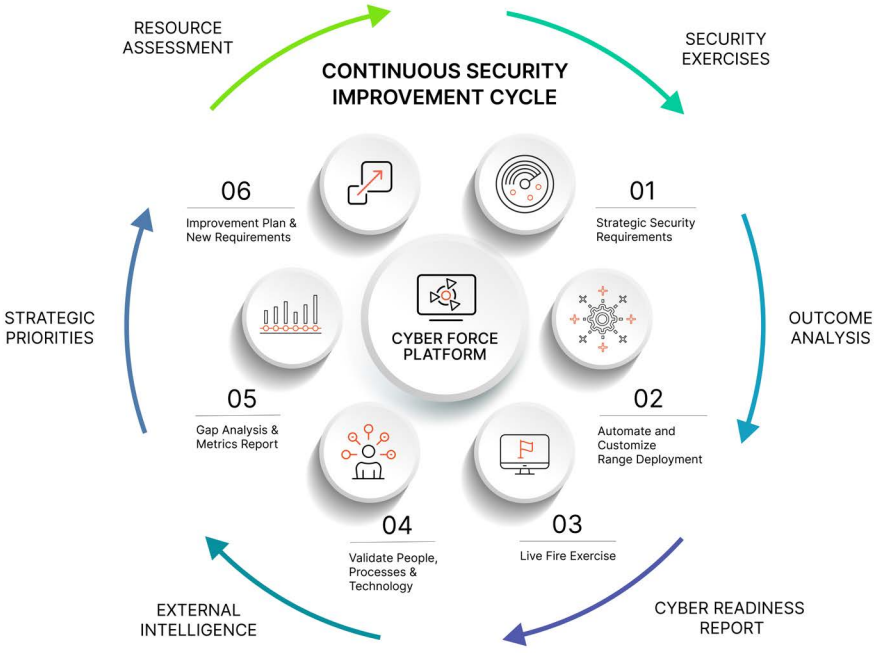
SimSpace provides a sophisticated, comprehensive, and scalable solution that can easily be tailored to fit our client networks and use cases.

SimSpace Cyber Force Platform strengths:

- Customizable, complex, high-fidelity training environments
- Hands-on cyber exercises, training, and assessment
- Candidate selection program
- Distributed create-your-own training and assessment plans
- Cyber combat skills contests
- NICE 3.0[1] mapping
- Integrated performance reporting
- Training marketplace
- Advanced capabilities:
  - Intelligent, host-based User Emulation (UE)
  - Sophisticated automated attack scenarios: Cyber Range Attacks For Training (CRAFT)
  - Zero-day emulator
  - Network replay & mission impact
  - Event tracker and planner for team-based events
  - Automated scoring

Solutions for Your Business

The SimSpace Cyber Force Platform is a distributed web-based application that provides the ability to conduct full-spectrum cybersecurity operations, including training, testing, and assessments. SimSpace allows you to generate, share, and participate in individual, collective, and force-level (team on team) training exercises as well as mission rehearsals, experiments, and certifications. SimSpace provides global, persistent access that enables users to develop and assess cyber capabilities, tactics, techniques, and mission procedures. With self-service platform access, SimSpace enables operationally relevant training in a reliable, realistic, secure, and reconfigurable environment — all on a standardized platform.



[1] NICE, National Initiative for Cybersecurity Education, has developed a framing of cybersecurity related skills/roles.

Sample use cases:

- Building individual and team readiness as well as maintaining skill levels
- Establishing a performance baseline and monitoring of improvements
- Learning new defensive tools at the team and individual level
- Testing and developing new red-team tools and TTPs[2]
- Evaluating and testing existing and potential new security products
- Rehearsing mission and tactics
- Conduction classic Red Team vs Blue Team[3] exercises

Available content:

- Over 700 hours of elite cyber-ops and threat-hunting team development content
- A number of sector-specific network environments are available out-of-the-box. Examples:
  - The financial services industry range comes with a payments application, point of sale systems, branch locations etc.
  - The mini power plant range contains an emulated OT/ICS environment
  - Other ranges like the town hall include custom applications that are more aligned to those industries
- Advanced, intelligent automated attack scenarios

SimSpace provides updates to the platform and content for all users with an active license on a quarterly basis.

Cyber Force Platform Offerings

Licensing and delivery options

SimSpace offers **Time Based Ranges** for one-off duration driven events and exercise engagements, **Persistent Ranges** for on-going readiness improvement, and **National Asset** Ranges to support complex national interest, critical infrastructure and large global service provider requirements.

The SimSpace Cyber Force platform is delivered via the following licensing options:

1 | SimSpace SaaS (hosted) subscription license offering, where the capability is delivered out of a SimSpace secure and highly-available data center.

2 | Software only (on-prem) subscription license where our clients provide the necessary compute resources.

3 | SimSpace Software Licence (on-prem) and SimSpace provided hardware bundles are available

4 | Combinations of the options above are possible, where a client wants to run an onsite environment of SimSpace and connect it to a SimSpace SaaS (hosted) version

SimSpace SaaS (Hosted)

The SimSpace hosted solution is hosted in either our data center in Boston, MA or our Frankfurt data center, in Germany. Within these data centers, the platform can operate either as a single-tenant solution on dedicated infrastructure or in a large multi-tenant computing environment. On this hosted solution, SimSpace staff handles all the physical security, racks, power, backup, internet connections, servers, storage, and networking. We also man the help desk and monitor for service availability and security. The hosted solution has been operating for over four years with over five million VM[4] hours of service at 99.9% availability.

[2] Tactics, Techniques, and Procedures used by malicious actors.
[3] Red Team versus Blue Team exercises are often used to simulate malicious attacks, with the Red Team acting the part of the attackers and the Blue Team serving as defenders.
[4] Virtual machine.

SimSpace SoftWare Only (On-Prem)

The self-hosted SimSpace Cyber Force Platform architecture leverages the VMware hypervisor[5], enterprise computer hardware, and enterprise-grade storage.

This traditional approach provides for isolation and self-routing to operate in customer premises and without reliance on Internet-based services. Traditional support services like chat, help desk, and technical operations manager are included in the platform and can be accessed within a user's profile.

Isolation means that the range environment is completely self-contained, with virtualized core routing infrastructure, a corpus of Internet representative content, Internet core routers, BGP[6] and root DNS[7], in addition to all internal infrastructure for any business or entities being represented in the experimental network design. Being isolated also allows the SimSpace Cyber Force Platform to maintain a real copy of a production network or for users to experiment with malware or other destructive techniques without concern of affecting real hosts or services. This provides enormous potential to create experimental network environments that are uniquely representative.

Extensibility is also easily possible for the hosted or on-premises version of the SimSpace Cyber Force Platform. Any service or appliance that can run on commodity Intel x86 virtual machines (VMs) can be included in a SimSpace range. Beyond these easily virtualized options, it's possible to attach and include external hardware with the rest of the range, which can include servers, devices, and even other specialized IP networks of interest such as an ICS network. Network interfaces on any of the range VMs can be routed to the external network to act as control or management consoles for the external devices.

SimSpace Software Only (On-Prem) License plus SimSpace provided Hardware (appliance/s) Bundle

To simplify the on-prem setup and integration, SimSpace can include hardware (appliance/s) with the software only licensing as a complete 'turnkey' bundle. SimSpace is then delivered ready to go with all necessary components pre-installed and configured. These include the hardware components (compute, memory, storage), the VMWare hypervisor, the SimSpace Cyber Force Platform, and an integrated Help Desk and Chat solution. An infrastructure monitoring solution (TechOps) provides insights into the health and status of the server and applications. Once delivered, the appliance simply needs to be set up in the rack and configured with the appropriate IP addresses. SimSpace can be operated in air gapped networks, in highly classified environments, completely disconnected from the internet.

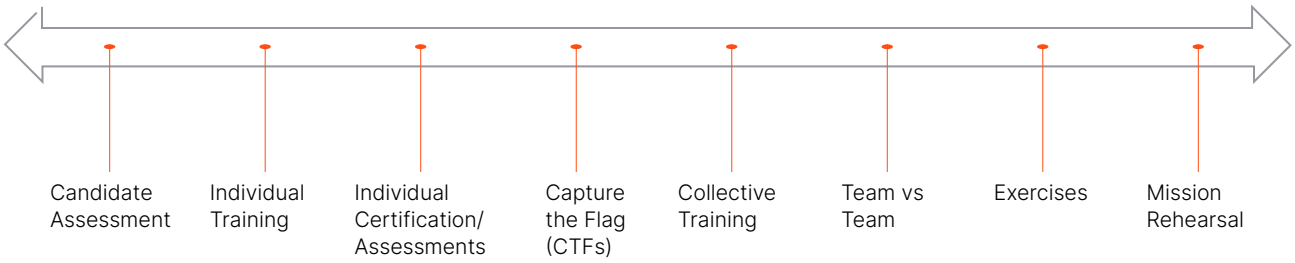
Being isolated also allows the SimSpace Cyber Force Platform to maintain a real copy of a production network or for users to experiment with malware or other destructive techniques.

[5] Software which allows one real host computer to support sharing its resources between multiple virtual machines.
[6] BGP (Border Gateway Protocol) is the network protocol used by the internet.
[7] The root DNS is a set of servers which host domain names and are essential to the internet as a whole.

Elite Force Training for Cybersecurity

The platform offers the ability to create and schedule individual as well as team-based events. Performance management capabilities enable training managers and "White Cell Leadership"[8] to analyze and evaluate organizational readiness using established frameworks like NICE 3.0 and the MITRE ATT&CK[9] framework in order to develop an actionable risk remediation plan. SimSpace's Learning Management System (LMS) and Content Management System (CMS) are found within the Content section, which provides training and assessments for both individual defensive and offensive operators as well as for defensive and offensive crews/teams.

The SimSpace Cyber Force Platform and its content provide a rich, full spectrum of training from identifying initial hires to sophisticated mission rehearsal.



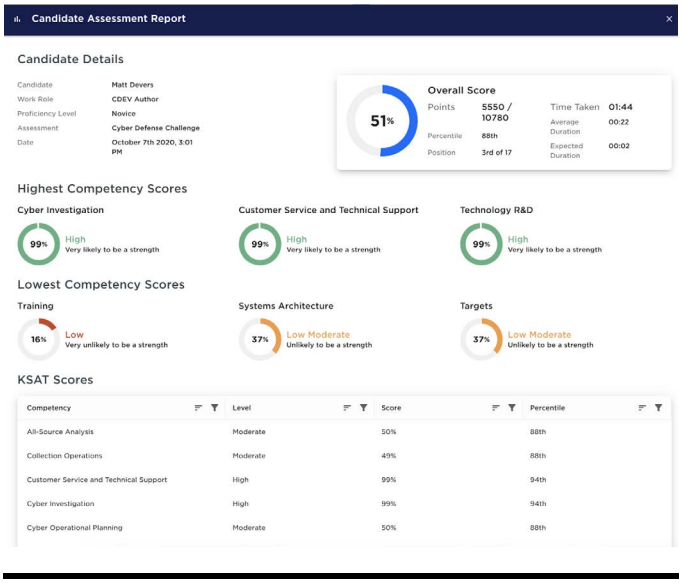
- **Hands-On Cyber Training and Assessments**
  Realistic, complex training missions set inside virtual networks; automated scoring; variability in the certification/assessment presentations; instructional materials such as short videos to enhance critical cyber concepts; content ratings and reviews
- **Content Authoring**
  Support for the development and integration of customer-generated training modules; selectable mission objectives; configurable NIST's NICE mapping
- **Training Marketplace**
  Support for hosting Cyber Range-based training modules from third-party vendors
- **Cyber Combat Skills Contests**
  Individual skills challenges go beyond typical gamification solutions
- **NICE 3.0 Mapping**
  Training modules mapped to the NIST NICE's Framework Job Specialties, Competencies, Tasks and Knowledge, Skills and Abilities (KSAs)

[8] Team responsible for overseeing both sides of a Red v. Blue training exercise.
[9] Global repository of information about cyber attack methods.

Candidate Assessments

The Candidate Assessment feature enables you to create a virtual test scenario for evaluating the capabilities of individuals who are not currently a part of your organization or a potential supplier like a managed security service provider. By providing candidates with isolated content designed specifically for evaluation purposes, this enables skill assessments to take place in a highly-realistic setting that is isolated from all other systems, minimizing security risk while gathering deeply meaningful information.

Assessments are conducted based on content created by SimSpace or by internal members of your organization. Individuals taking an assessment are scored using a combination of questions and answers as well as “In Range” assessment, where the candidate is immersed in a virtual environment as large or as small as (and as detailed as) the organization requires for the evaluation. Proficiency scores are calculated based on successful completion of the questions and tasks, time to completion, response attempts, and number of hints taken.



A Candidate Assessment Event is created and launched only when the external user for which the Event is designed is ready to begin. The Candidate accesses the Event via a designated URL constructed specifically for that Candidate and is available for only a specified time. All resources required for the Event, such as virtual machines, networks, and other assets, are provisioned only when the Candidate chooses to begin the Event, and are available to them for only as long as that Event is active for that Candidate. The Event ends as soon as the Candidate completes all tasks, explicitly ends the Event by canceling it, or the time allotted for the Event expires.

After the Candidate has completed the Event, the hiring manager and other interested parties in your organization can review how that person performed. A detailed report reveals, at a glance, the overall score and percentile for the Candidate and their three highest and lowest competency areas, along with scores and percentiles for each part of the assessment.

Individual and Team Assessments

Individual assessments are conducted by using either organic or third-party content for existing team members or new candidates. Once an individual starts an assessment module, they are scored using a combination of questions and answers, or automated assessment of keyboard input. Proficiency scores are calculated based on successfully completing the questions and tasks. Factors like time to completion, number of attempts at answering a question, and the number of hints taken is recorded.

Team-based performance is assessed using a multi-user Cyber Range where group performance is measured against the training scenario goals, objectives, and tasks.

Team-based scoring leverages information from the following sources:

- The scenario goals, objectives, and MSELs specified in the training package
- Output from the attack injects/MSEL[10] tracking tool
- Results from the automated OPFOR[11]) actions
- Results from the MITRE ATT&CK framework mappings
- Team responses in the Content application

Participant responses, along with team documents and After Action Reports are stored for team performance and analysis, for recordkeeping and reporting of overall team performance and readiness.

The SimSpace Cyber Force Platform provides a high-fidelity, automated environment for the development and testing of new products and capabilities.

[10] TMSEL (Master Scenario Events List) is an outline describing the sequence of events participants will undergo during a training
[11] OPFOR stands for 'opposing force'

Testing

The SimSpace Cyber Force Platform provides a high-fidelity, automated environment for the development and testing of new products and capabilities. Complex, tailorable network environments with real security tools and policies, highly realistic host-based user traffic, rehosted Internet sites, automated intel-driven APT attack scenarios, data collection, and scoring are all capabilities that can be brought to a test to quantitatively assess the performance and capabilities of new products.

Example use cases for product testing include:

- Development
- Demonstrations
- Evaluations
- POCs
- New tactics, techniques, and procedures (TTPs)

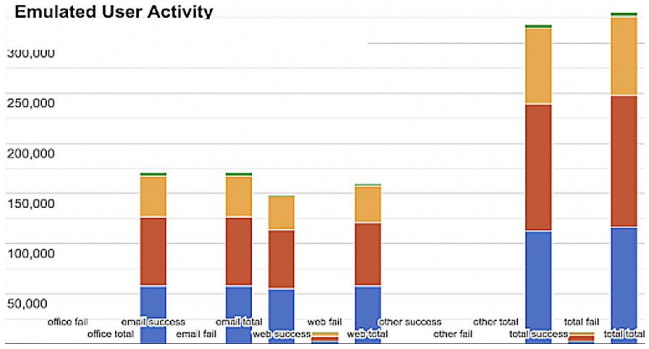
Product testing

Independent tests of cybersecurityproducts

- Tailored network environments
- Tailored attack scenarios
- Instrumented environment
- Test harness for control and analysis

Measure product effectiveness:

- Time to setup
- Ability to detect attack scenarios
- Time to notify
- Usability
- Overhead on host machines
- Impact to virtual users



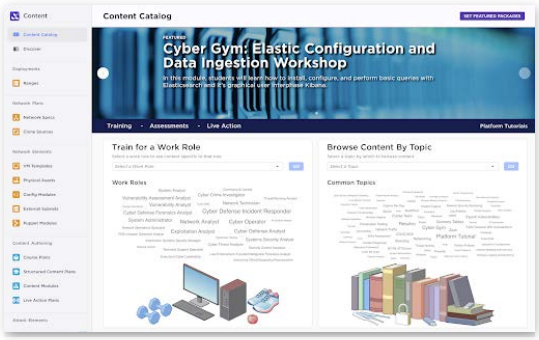
Security tool impact to virtual user operations

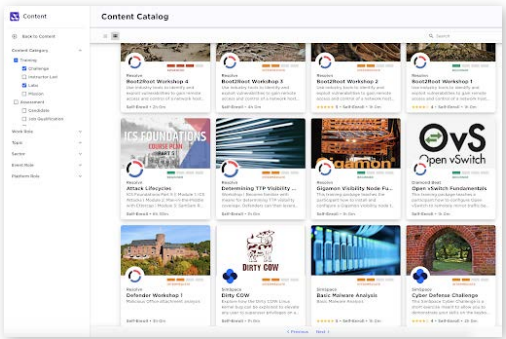
Content Catalog

The Content Catalog provides users the ability to discover training and assessment content that has been published by content authors (SimSpace and its partners) for general consumption. Third-party content can also be published and scheduled via APIs provided by the platform.

SimSpace content encompasses training content for many roles. Some examples include:

- System Analyst: Conducts host-based artifact collection and forensics to detect and analyze indicators and warnings of adversary intrusions on a defended network. Evaluates the security posture of endpoint devices and makes recommendations on ways to mitigate security vulnerabilities to specific adversary threats.
- Network Analysts: Conducts collection on network traffic using data derived from sensors, intrusion detection systems, and logs from network devices. Uses this data to detect and analyze indicators and warnings of adversary intrusions on defended networks.
- Network Technician: Provides expertise on the security posture of a defended network's routing and switching devices, firewalls, and network proxies.
- Cyber Threat Intelligence Analyst: Provides prerequisite experience in All-Source Intelligence and tailors that experience toward the analysis of cyber threats and intrusions. Cyber Threat Intelligence Analysts must be familiar with the fundamentals of technical cyber threats and intrusions.
- C2 Element: Consists of mission leaders or defensive team leads. Responsible for traditional Command & Control (C2) roles but is also responsible for ensuring that a mission element adheres to cybersecurity policies, procedures, regulations, and statutes while on mission (avoiding violations).





The Content Catalog comes with the ability for content authors to discover, create, and manage content across the platform. Content is available from SimSpace and third-party industry experts and can be used as is or can be created and tailored for the organization. In each area, users can create and add to the library with their own material.

The Content Catalog includes:

Library
All published training and assessment content is ready for users to consume

VM Templates
Templates used to create VMs in network ranges

Recently Added
The most recently added content

Config Modules
Range automation modules, including puppet modules

Ranges
Network ranges and deployments

Physical Assets
Hardware owned and available for use by an organization

Network Specs
Network specifications (blueprints)

Content Modules
Collections of tasks and questions that can be used in Structured Content Plans

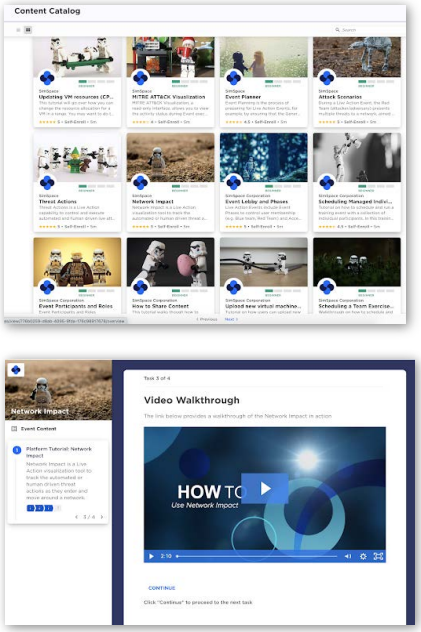
Structured Content Plans
(Training Packages)
Collections of Content Modules, used in Events

Clone Sources
Copies of deployments that can be used to quickly bring up multiple copies of a range

Attack Scenarios
Library of automated and manual attack scenarios

Platform Tutorials

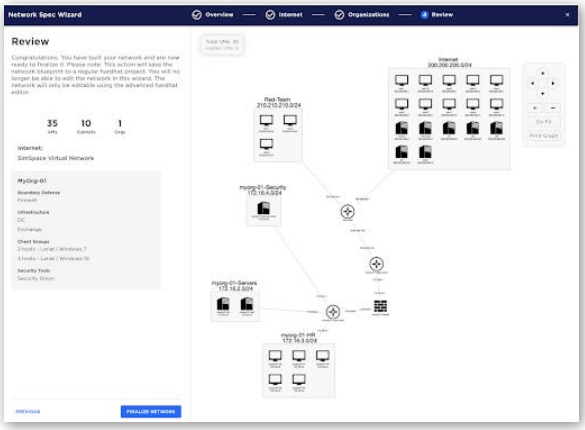
Within the catalog are a collection of tutorials to provide an overview of the platform capabilities and a short video walkthrough. These are intended to help new users come up to speed with what the capabilities provide and how to use them. We've also added tutorials with detailed walkthroughs for tasks requiring significant technical knowledge or knowledge of SimsSpace technology.



Network Specs

The Network Specs section is a collaborative interface for designing networks to be used within a SimSpace Cyber Range.

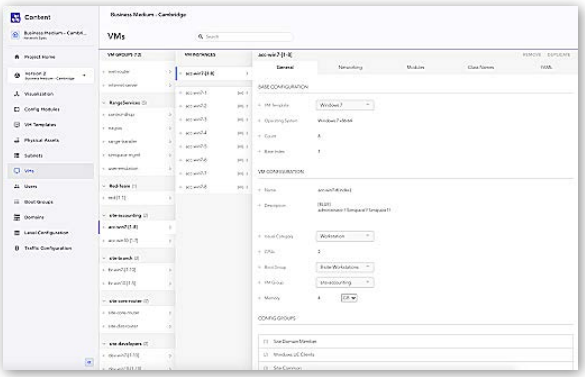
Using the Network Specs visualization tool, users can define hundreds to thousands of VMs in a high-level format that supports identifying the specific configuration for the individual machines that are key to the virtual network. Additionally, Network Specs supports a rich configuration syntax to install and configure the necessary applications and services within the environment. The Network Spec includes information and details about the network topology, hosts, services, virtual users, traffic patterns, along with the automation modules used to define and automatically build the network.



Network Spec Wizard

The Network Spec Wizard allows for the creation of a network specification through a series of web forms. As the range is being designed, an updated network map of the environment is created. The end result is a network specification that is ready for deployment or further customization.

Using the Network Spec Wizard and Network Spec deployment tools, a brand new complex network environment with hundreds of VMs, services, host-based traffic generators, security tools, and infrastructure can all be automatically built out in hours, compared to the weeks it would take to build out manually.



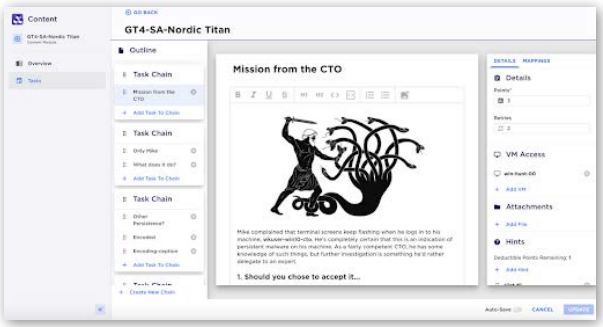
Virtual Machines and Security Tools

SimSpace provides an initial collection of base operating systems and tools to work with. These include the Microsoft operating systems and applications, open-source software like Ubuntu, Kali, and Vyatta, as well as some commercial products like Splunk[12]. One of the goals for the Cyber Range is to replicate the systems and tools used in production environments so we offer users the ability to load and configure their own tools. Some examples of security tools we have used in the range are in the picture below. SimSpace provides the ability for users to upload new virtual machines and, if required, obtain approval from a manager or security team before making them available in the Content Catalog for general use. SimSpace allows for the integration of both virtual machines and physical appliances into its Cyber Ranges.

[12] Splunk is a popular software package used for analyzing complex machine-created data through a web interface.

Content Authoring

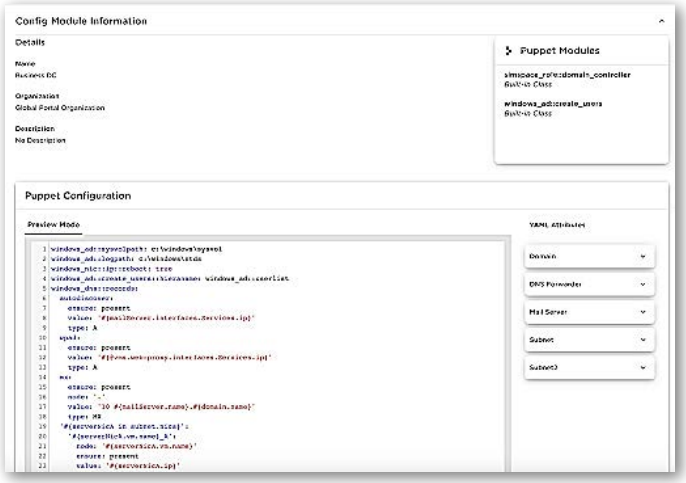
Content authors are able to create custom training modules or adapt the existing ones for their organization's needs. Using built-in tools, they can format rich multimedia content with videos, images, documents, and associations to appropriate virtual machines. They can map content to the NICE Framework to enumerate Knowledge, Skills, and Abilities competencies supported by the material, and use hints and complex point assignments for questions. Images, documents, and videos can be embedded in the content. The virtual machines used in the training can be created with the network designer and provided attack tools to give hosts all the desired artifacts for the training. Once the training package is created, the author can share it with members of their team or others in their organization.



Config Modules

Configuration modules allow you to automatically install, initialize, and configure the virtual machines, applications, services, and tools in your network. Puppet[13] and Ansible[14] are the automation frameworks used to configure the systems in the range. The Content Catalog comes pre-populated with over 100 puppet automation modules for configuring systems and tools in the range, including those for installation and setup of domain controllers, exchange servers, file servers, host-based user agents, host monitoring tools, DNS, firewalls, and routers.

The provided puppet modules can be extended by users, who can also add new ones. An example of a puppet module in the Content Catalog is shown here.



Configuration modules allow you to automatically install, initialize, and configure the virtual machines, applications, services, and tools in your network.

[13] Open source tool for configuring and managing software - Puppet allows users to 'pull the strings' on multiple servers at once.
[14] Ansible is a tool for automating common IT tasks which are particularly cumbersome.

High-Fidelity Tailored Environments

Range Buildout (Orchestration)

Network environments require a sufficient degree of complexity and breadth to ensure rigorous testing. This in turn requires the ability to quickly create new environments, either by custom-creating a brand new network environment to your own specification, or by selecting a network from a catalog of predefined networks, then expanding or modifying it to suit your needs. These predefined networks vary in scale from tens to hundreds of nodes and are representative of a variety of organizations, such as enterprises, defense industrial base companies, financial institutions, utilities, and military networks. These virtual networks are all self-contained and isolated from the Internet in order to prevent any accidental spillage or inadvertent attacks on real-world sites or assets.

Our intent is to provide a safe environment for research, development, testing, and exercises without compromising on environment fidelity. Despite the advantages of being isolated, effective testing and training often still require a realistic Internet experience. To accomplish this, thousands of sampled web, email, and FTP sites are re-hosted inside the range. Root and domain DNS servers, as well as core BGP routing, are also provided. The range additionally contains fully functional representative elements of a typical network, including routers (virtual), full Windows domain controllers, Microsoft Exchange and IIS, DNS, and file servers. Linux, Unix, and other server and client operating systems are also included, along with “mimic” sites which are intended to imitate social networking and cloud services.

Real-world networks are rarely perfectly constructed and aligned, given the reality that there are often many misconfigurations and idiosyncrasies included in them, in addition to legacy and unwanted traffic. These elements are factored in to represent what a system administrator would come to expect from a typical real-world environment. The SimSpace implementation of User Emulation sets up personas that enable virtual users to interact with content in a realistic manner (e.g., send/receive/open email attachments, click on embedded URLs, etc). A wide range of operating systems, services, data, and user accounts is possible due to our extensive development of the tools and processes which fully automate both the setup and configuration of our systems.

The process of automated range configuration and setup of clients and servers includes the loading of accounts onto servers and setting up content, along with configuring client machines, applications, and server setup (e.g., domain controllers, web servers, Exchange servers, file servers).

To support automated range design, deployment, and configuration (range orchestration), SimSpace has built a suite of custom tools to rapidly define and automate the range setup. This includes leveraging the tools in the Content Catalog which include the Network Specs, virtual machines, physical machines, range host automation scripts (e.g. Puppet, Ansible), and network segments.

Simulated Internet

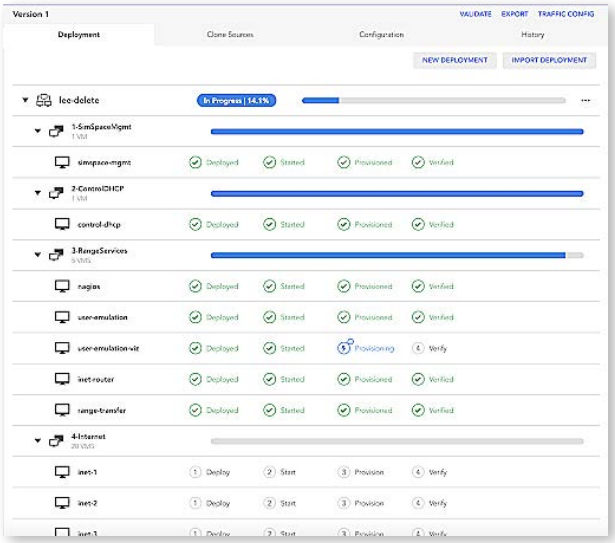
In order to provide a realistic network environment, each virtual network includes a simulated internet infrastructure to provide a high-fidelity environment to mimic operational networks.

The simulated internet system provides:

- Root domain name system (DNS) services
- Cached copies of real-world websites
- Interactive websites for blogging and social media interactions (similar to Facebook)
- BGP-based wide area network with one or more virtual ISPs
- Emulated Internet users
- Threat presentation (OPFOR) tools

File Management

The File Management feature within our Live-Fire Experiences provides visibility into file history and allows for a more flexible and reliable file transfer experience. Users are able to upload files to our Cyber Range and generate a download link. Additionally, there is a Download History View that displays which files have been used in the Range associated with the Live-Fire Event.



User (Activity) Emulation

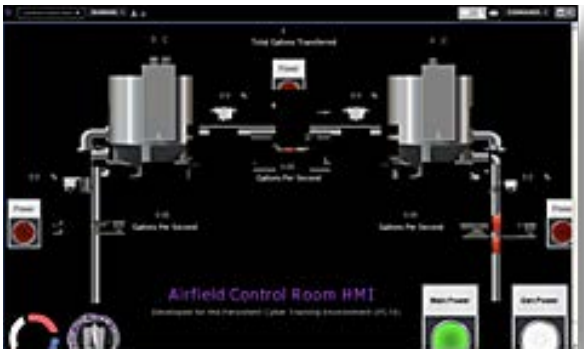
The SimSpace Cyber Range features an integrated User Emulation system that imitates the behavior of different types of enterprise users by controlling common applications on each user's hosts to achieve that user's customized goals. The simulated users generate user interaction with applications, web sites, and other servers which then drive network traffic. This results in a realistic simulation of an enterprise network of users that are actively working and connecting within the network.

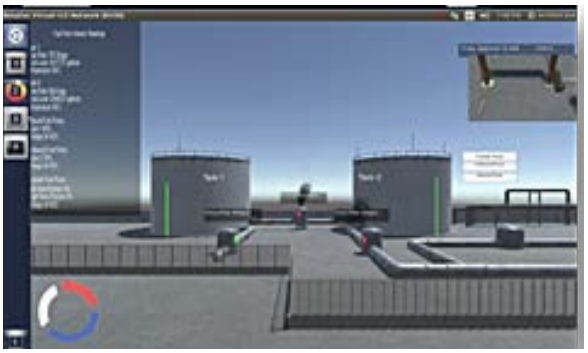
Realistic environments exhibit some level of chaotic activity, which User Emulation can reproduce to make each simulation statistically similar, but not identical. Each simulated agent is configured to adapt to changing conditions in the environment, and will take other actions as needed to respond to environmental changes. Additionally, a simulated user could be scripted to provide deterministic behavior every time, such as to emulate insider threat actions at specific times. Packet replay tools cannot match the representative, varied, and adaptive behavior presented by the Cyber Range.

User Emulation creates personas that govern a group of user's actions such as the websites they visit, the people they email, and the amount of time they devote to different activities. Extensive customization of a user persona is possible by specifying how and when the user spends their time each day. For example, one class of users may spend 30% of their time reading and responding to email, 40% of their time creating documents and spreadsheets, and 30% of their time interacting with websites. Many of these activities can be further refined, such as by providing a corpus of other users to email, or of certain websites to browse. Additionally, the number of concurrent users and the speed with which users start new actions can be adjusted to achieve a desired activity load on networks and servers.

Simulated users can engage with a variety of common business applications, and the User Emulation system can be modified to handle nearly any application. Users can browse websites, follow links, and interact with dynamic web applications on modern browsers. They can create new documents and open existing documents with the Microsoft Office suite. They can send and respond to emails, including being able to interact with attachments and links in them. Sharepoint servers can be used for collaboration; command line (SSH) clients can access remote SSH servers and execute remote commands. In short, User Emulation provides realistic security-related noise such as opening email, browsing to malicious websites and clicking on links. This allows attackers to hide their actions within the environment and forces the defensive team to take note of all manner of potential adversary actions.

The network library includes domain-specific environments like business, financial services, military, government, and power company networks, with specialized and domain-specific applications that operate in those networks (e.g., financial payment systems, Automated Teller Machines (ATMs), HVAC, oil and gas simulators). Screenshots of some HMIs and simulators for a bespoke refinery range are shown below.

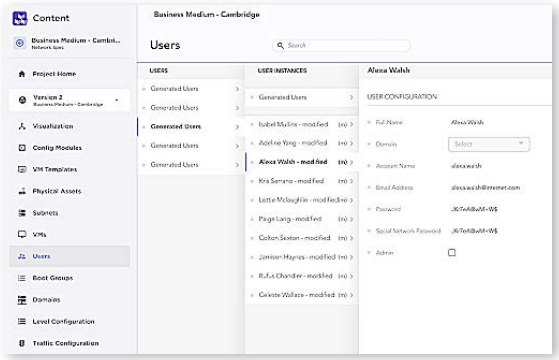




Unique user personas with custom behavior profiles are automatically generated during network creation

Wormhole

Comprehensive testing of defensive posture should exercise real-time detection of (and responses to) adversaries already inside the network, and be repeatable in the Cyber Range environment. The challenge is consistently replicating a zero-day exploit behavior that allows adversaries to bypass current antivirus, firewall, and intrusion detection systems. Wormhole is an operating system service that mimics the effect of a zero-day attack, providing a method to bypass network defenses and get a foothold inside the network.



Cyber Range Attacks for Training (CRAFT)

To model sophisticated adversary behaviors and actions or Advanced Persistent Threats (APTs), SimSpace has developed automatic attack scenarios called the Cyber Range Attacks for Training (CRAFT) capability. CRAFT is an automated attack scenario framework that models all the phases of an attack scenario, from initial compromise and lateral movement around the network to going after a specific target in the network and setting up the command and control channels. Data exfiltration and post attack actions such as cleanup are also included. CRAFT uses real-world attacks and tools and works with FireEye to provide the latest real-world intelligence for modeling specific threats. CRAFT also leverages the Wormhole zero-day emulator to gain access on a host and evade defensive tools.

SimSpace currently provides over a dozen ready-to-go automated attack scenarios like APT3, APT10, APT40, Beaconing, Exploitation of a Domain Controller, and reconnaissance scenarios. These scenarios use a multitude of specific attack tools and exploits as they execute throughout the networks. SimSpace provides all of the CRAFT scenarios on specific networks so users can simply start up a training scenario and everything is ready to go.

The attack scenarios are intelligent, using an orchestrator with AI and machine learning to adjust their actions and attack paths with alternate tools and techniques if it detects changes in the network or defensive actions. Randomization is used through the attacks to target equivalent sets of machines, maximize reuse, and allow teams to re-run the same attack scenarios without knowing in advance what the attacks will do.

A bypass capability has also been developed to allow the automated attack scenarios to advance to the next phase if they are blocked and no other options are available to the attacker and orchestrator. The bypass allows a team to get the full value out of a training scenario, though from a scoring perspective, it would be noted that they would have been able to defend against this scenario. As an example, if an initial spear-phishing email were blocked or not delivered to the target user, after some period of time the orchestrator would bypass the defense and continue the attack as if the user had opened the email.

As the automated attack scenarios execute on the network, their status at each phase is posted to the Event Historian so their progress can be visualized on a network map (Network Impact) and the techniques and procedures being used can be visualized using the MITRE

[15] APT stands for Advanced Persistent Threats, which follow their targets over long periods: months or years.
[16] Beaconing refers to regular communications sent by a system infected with malware to a server owned by a hostile entity.

ATT&CK framework. This information is also used by the scoring engines to automatically assess team performance based on the completion of objectives and other predetermined factors.

These complex attack scenarios are typically created to mimic the actions of a live red team. The same attack can be repeated in a controlled fashion in other network environments or while varying experimental parameters. This type of regression testing is powerful because the unit of test is a full, complex attack scenario. Testing different defensive teams against the same attack sequence in the same network environment allows for direct comparison of team performance. This leads to a deeper understanding than possible with a live red team, given the inherent variability of human actions. Evaluating defensive products through A/B testing is also possible by running a suite of automated attack scenarios against a new product to compare performance with existing defensive products or other competing products. This level-setting of performance allows you to move beyond vendor performance claims by understanding how tools compare under the same realistic attack conditions within a model of your environment.

Some classes of testing benefit from keeping the network environment, tools, and teams constant while only varying the nature of the attack. SimSpace CRAFT supports modifying the behavior of attack scripts during execution by varying the time between attack steps and forcing mistakes in the adversary workflow (e.g., mistyping commands in remote shells, incorrect binary for the target platform). This allows a single script to simulate a high-skill adversary with fast execution of steps and no mistakes, a low skill adversary with longer thinking time between steps and mistakes in remote shell commands, or any skill level in between.

SimSpace is developing new attack scenarios, additional attack tools, and more realistic AI models of user behaviors for each quarterly release, providing a growing and up-to-date library of attack scenarios to train and test against.

SimSpace is developing new attack scenarios, additional attack tools, and more realistic AI models of user behaviors for each quarterly release.

Events and Exercises

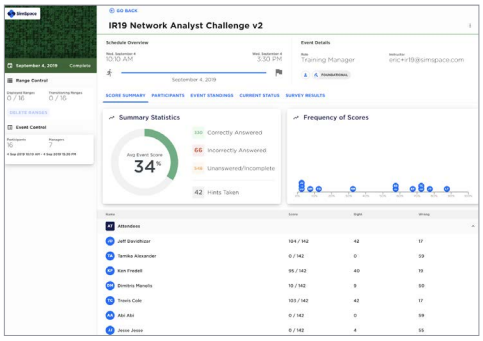
The Cyber Force Platform training is structured around two primary event types:

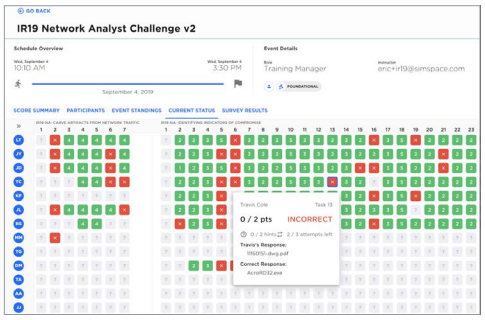
- Structured Content Events and Exercises: Individual and team lab training, primarily used to build and test skills
- Live Action Events and Exercises: Coordinated, live, team-based events that pit defenders (Blue Team) against attackers (Red Team or automated attacks)

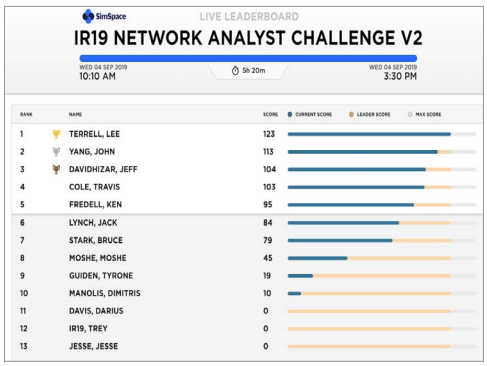
Structured Content Events

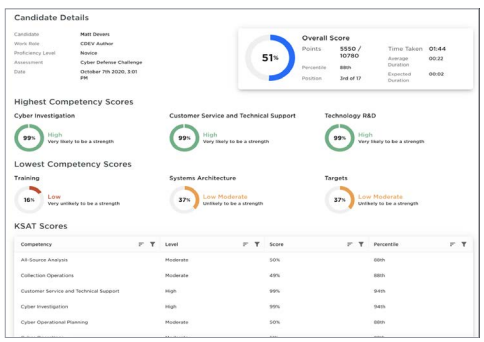
Structured Content Events are training courses designed to teach a wide variety of skills to teams and individuals. They also allow for skills assessment and detailed monitoring of progress. These events are content specific and challenge users to answer relevant questions. Training Managers create and schedule Structured Content Events. In addition, they can view both individual course progress and all performance results. These Events can also be configured to run as self service so that users can schedule a lab without requiring a manager or team lead's involvement.

A manager who schedules a lab for a set of users will be able to view each member's status and progress in the lab to see how they are performing and provide assistance as necessary. As users progress through a lab, points are awarded for answering questions correctly and deducted for use of hints. A team-wide leaderboard is available for competitive events, showing which team members have earned the most points. Structured content is mapped to the NICE 3.0 Framework so that individual knowledge, skills, and capabilities can be computed for each member. Results are available to be viewed individually by members, and for their managers to see how they are doing compared to others.









Live-Fire Events (Exercises)

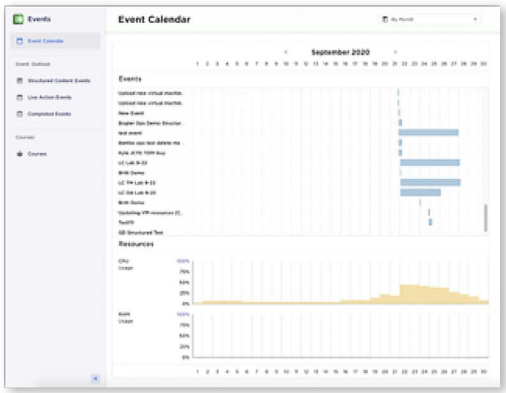
Live-Fire Events use complete ranges or networks with live clients, servers, and security tools running in the network. In this environment, live defenders go up against live or automated red teams. These events may include goals and objectives for the team to work toward, with customization and tailoring of the network, tools, and attacks for the event. Live-Fire Events unfold over a series of phases, so teams are provided access to the environment prior to event execution, should they need to add any components to meet the goals of the event design.

Event Phases and Execution

Live-Fire Events allow an Event Manager to manage access and control of the applications (e.g., Attack Controller, Network Impact) for each user role (e.g., Red Team, Blue Team) during each of the event phases. The event phases provide a logical transition through Event Design, Setup, Blue Reconnaissance, Red Reconnaissance, Execution, Assessment, and finally, Post Event. Each phase grants different team members access to the event range, and each member gains certain capabilities based on their event roles. Event Managers can customize which roles get access to that application for each event phase.

Event Calendar

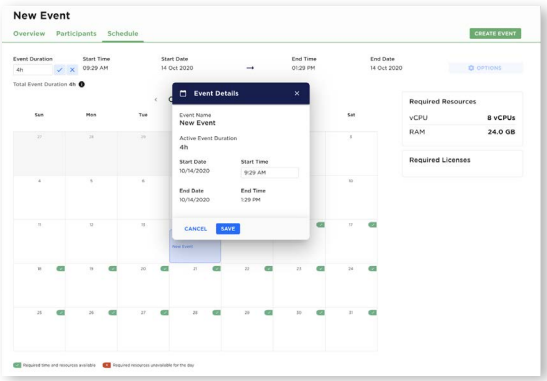
The Event Calendar allows Training Managers and Event Designers to view all scheduled events and corresponding resource usage. The events can be viewed as a Gantt graphical chart with associated resource usage. The visualization feature allows them to make strategic scheduling decisions, promoting efficiency.



Scheduling

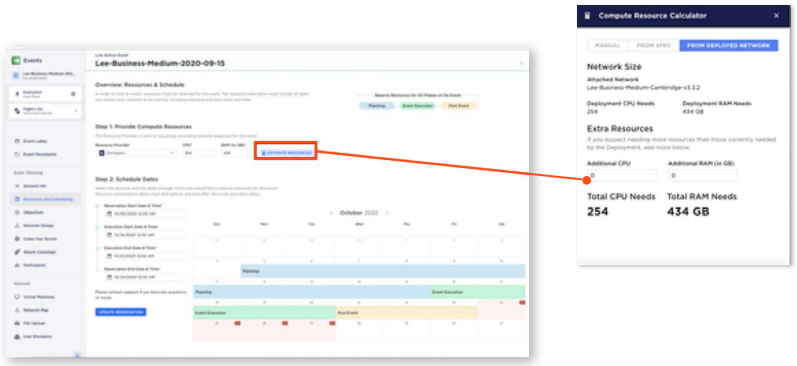
Structured Content Events

When scheduling Structured Content Events, typically used for individual training, available dates can be selected in a calendar view. Based on the lab resources (such as amount of CPU and RAM) being used and the number of users, the scheduler computes the total resources required to execute the event and shows dates when these resources will be available. For self-service labs, the scheduler performs a check to make sure the chosen date and time is available. When an event is completed or the time reserved for it elapses, all ranges associated with that event are deleted to conserve resources and returned to the pool of available resources for other events.

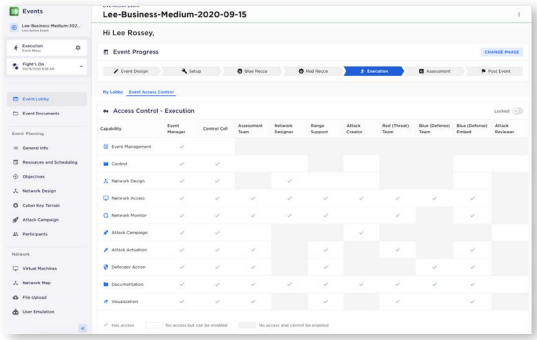


Live-Fire Events

A similar scheduling process is performed for live team-based events. For these, however, range use is defined over a series of phases (Planning, Execution, Post-Event). A scheduling tool helps Event Managers allocate the required resources, as the ranges necessary for live-action events are typically much larger than those used in structured content events.



Live Action Event Scheduling

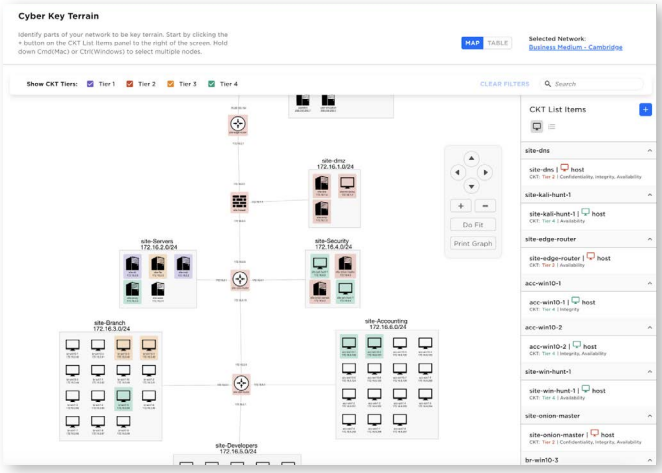


Cyber Key Terrain

Cyber Key Terrain (CKT) allows event designers to label network resources based on both the importance of that resource within the network as well as the impact of a breach against that resource (host/file/service). You can label resources along two dimensions — Tier (importance of resource) and Type of Breach (attack focus), which are Confidentiality, Integrity, and Availability (CIA) of data.

For example, labeling a resource as Tier 1 (Confidentiality) may indicate that the impact of disclosing the resource is organization-wide. Modifying or destroying an Integrity resource may have a lower Tier 3 designation, impacting only a segment of the organization.

Live-Fire Events are scored based on the objectives and the team's ability to protect network resources as specified by the Cyber Key Terrain.



Attack Scenarios

During a Live-Fire Event, the Red Team (attacker/adversary) presents multiple threats to a network, aimed at accomplishing goals such as exfiltrating sensitive information or disrupting essential business operations. Attack Scenarios prescribe how these threats are implemented. The "how" is specific to the MITRE ATT&CK® framework, a free knowledge base that contains attack strategies used by several industries, including the federal government and IT companies.

The Cyber Range comes with a series of predefined automated CRAFT scenarios, but you can also reuse manual scenarios that others have used or shared, or create your own manual scenarios from scratch. Attack scenarios are described as steps, with each step correlating to a Tactic-Technique pair from the MITRE ATT&CK framework.

Defender Logs

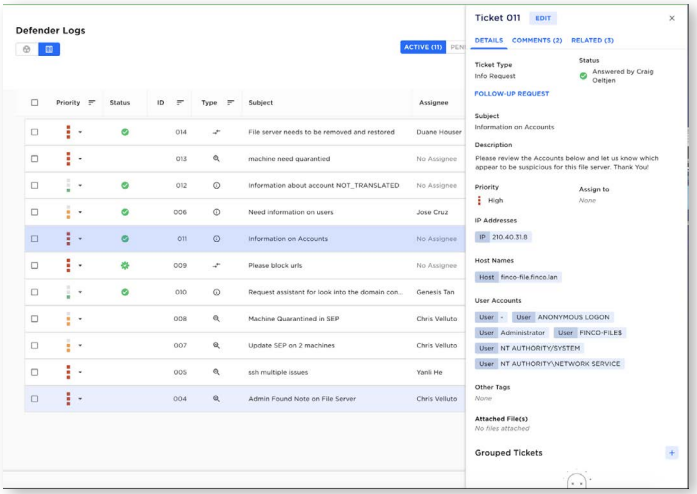
Assessments are most useful when the results are quantitative, because the performance of defensive teams or tools can then be meaningfully compared to historical trends in order to track performance improvements. Quantitative assessments require detailed recording of attacker and defender intent, actions, and effects, and in some cases, human observations of team interaction. This requires instrumentation of networks, devices, and servers, but also requires instrumentation of defensive personnel and processes.

The Defender Logs allow for participants to record actions performed by defenders during an event. These defender log tickets help to provide precise logging and timing while allowing the event coordinators to record observations and evaluate performance.

The Defender logs are critical for tracking and sharing of information during a Live Action Event. There are three types of defender log entries:

- Tracking Item – Information regarding detected activity
- Information Request – Clarification queries submitted to White Cell
- Change Request – Defensive team requests for changes to a network host in response to detected adversary incursions

Defender log entries are used for scoring, later in the Assessment phase.

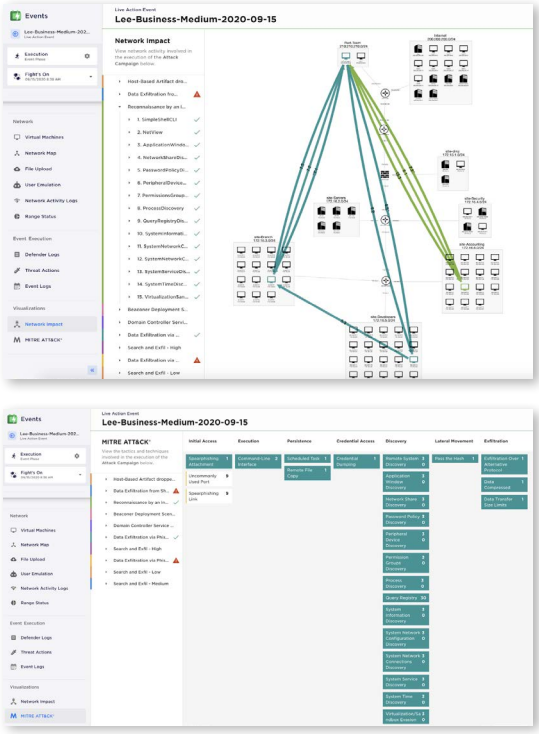


Range Access

Once users are granted access to the range, they see a list of available VMs, either in a table view or a network map, with their level of access based on their role (e.g., Red Team, Blue Team, Assessors). For each VM, they have full-screen interactive console access, the ability to copy to and paste from in-range VMs, and other VM management capabilities such as creating snapshots of individual VMs (admins can snapshot the full network) and uploading new VMs, files and other data into the range. Multi-user VM console access is also provided for either collaborative sessions or incognito monitoring (such as by managers and white cells).

Network Impact and MITRE ATT&CK Visualization

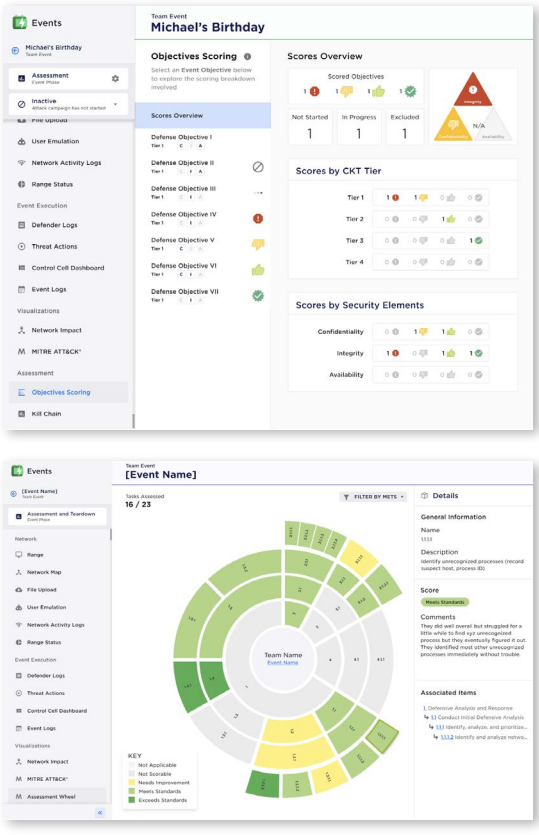
The Network Impact view allows users to follow threats on a network map as those threats enter and move around the environment. As each attack is started using the Threat Actions attack controller, it is tracked in the Network Impact visualization. The MITRE ATT&CK visualization allows users to follow the techniques and tactics employed by threat actors as they enter and move around a network



Network Impact view

Team Assessments & Scoring

Automated scoring is computed based on the objectives set for an event, their threshold criteria, the Cyber Key Terrain, the success or failure of attack scenarios, and the defensive actions taken by the Blue Team. Assessments for teams are based on the Measures of Performance (MOPs) and Mission Essential Tasks (METs). Visualizations show team performance and can be used for the reports and debriefs.

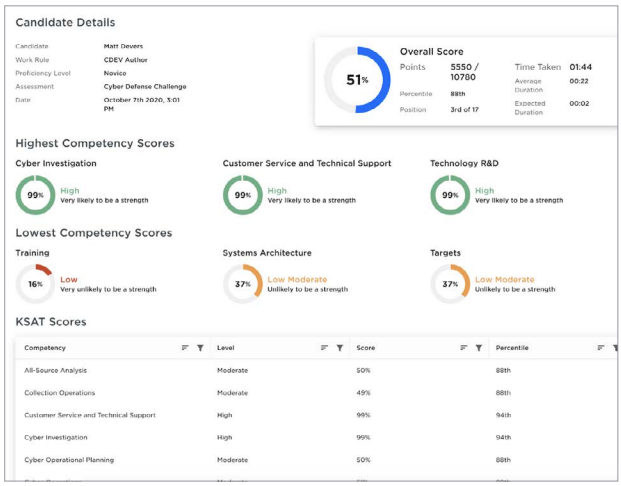


Measures of Performance (MOPs)

Reports and Analytics

Individual Performance & Readiness

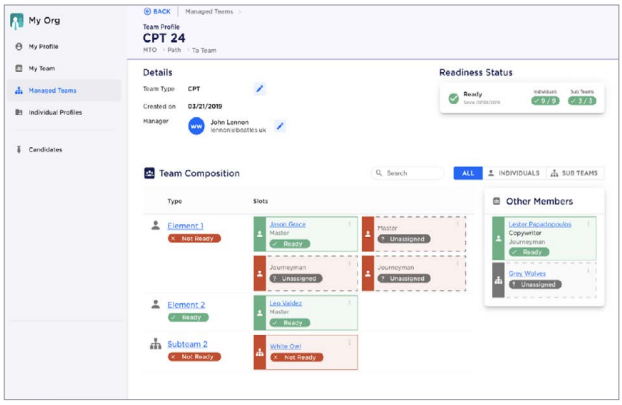
As individuals complete events, their scores and performance are calculated based on the NICE 3.0 framework. These are shown both to the individual and their leadership. Individual performance can be compared to others on the team or organization so that managers can identify those with the highest skills and those with gaps in their knowledge or competency.



In order to meet certification requirements, a member must receive a score in each test or Event that meets or exceeds the proficiency threshold set for that assessment. Whenever a member successfully completes an Event, their performance in that Event is added to their profile so their certifications are easily accessible.

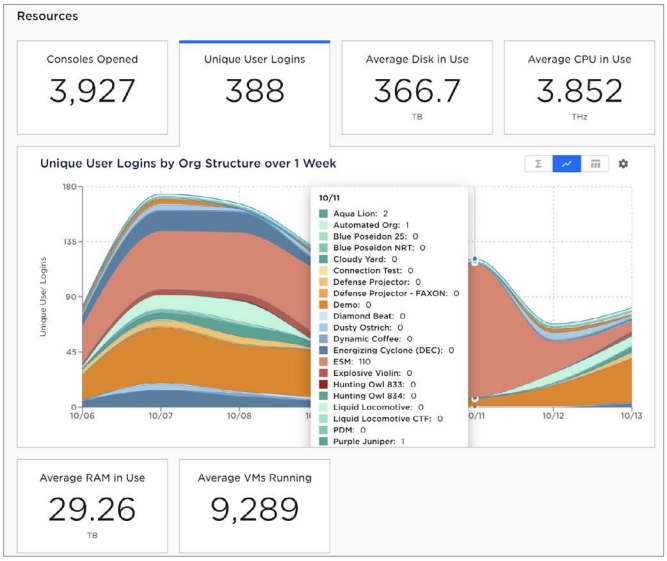
Team Performance and Readiness

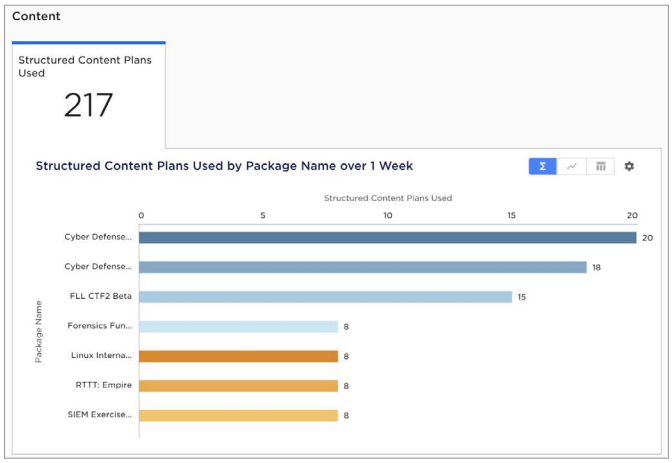
Teams are defined by the creation of roles with specific requirements for each role and assignment of users to roles. A member's certifications must meet or exceed the requirements for their assigned role and must not have expired in order for that member to be considered "ready" by the system. The Team Profile page displays the composition of the team by role, along with the certification status of each team member. When all members of a team are in a "ready" state for their assigned role, that team is considered "Mission Ready." These views are intended for leadership to understand how prepared each team is to perform its job.



Resources and Content-Use Analytics

The Analytics page provides metrics regarding the consumption of resources and content across the organization. Resource metrics include consoles opened, unique user logins, average disk, CPU, and RAM in use, and average number of VMs running. The content metrics show which structured content (training packages) have been used. This information can be analyzed over configurable timeframes (e.g., one day, one week, one month, three months, etc), filtered, and grouped by organization and sub-organizations to see which members are active as well as what they are consuming and when.





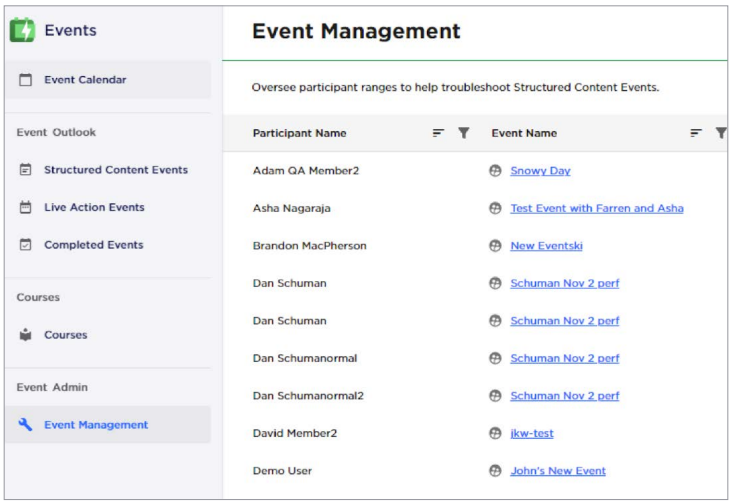
Resource metrics include consoles opened, unique user logins, average disk, CPU, and RAM in use, and average number of VMs running.

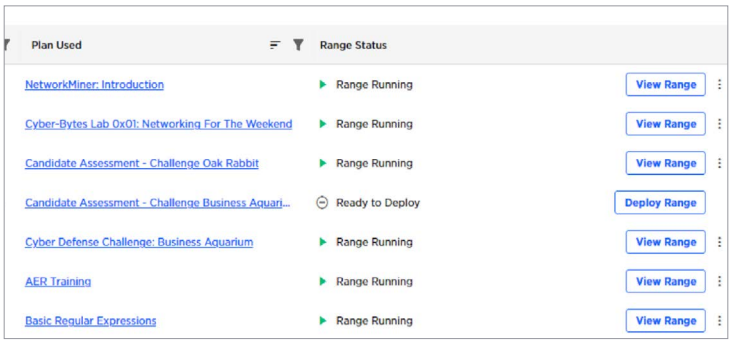
Troubleshooting

Resources and Content-Use Analytics

Event Managers and those in Administrator roles can use the Event Management dashboard to deploy, view, and troubleshoot a Range within a Structured Content Event.

Each event's range console page displays information at the virtual machine level, including number of users logged in and power state. For running VMs, an Event Manager/ Admin can log into a console within the Range for further troubleshooting.





Administration and Security

The Admin section is where authorized users manage organizations, hierarchical structures, users, roles, resources, content sharing, and security.

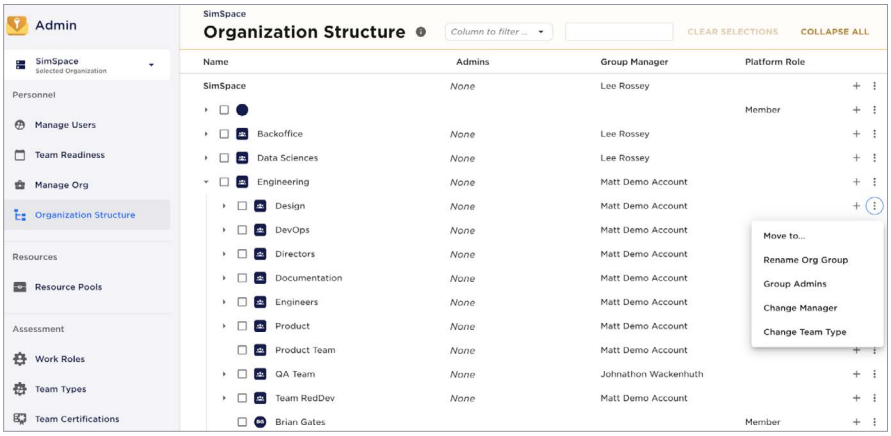
Resource Management and Scheduler

The Resource Manager allows administrators to define resource pools to allocate resources across the platform, and also to groups of users within an organization. The resources which can be managed include infrastructure items (CPU, memory, disk) and content licenses. When events are planned or initiated, the Scheduler ensures that resources and licenses are always under control and that all events can run as planned without resource conflicts.

Enterprise Account Management

User accounts can be managed locally or integrated with enterprise account management solutions using SAML, LDAP, or KeyCloak. The accounts can be organized using a Multi-Tiered Organization (MTO) structured to model organizational hierarchies (e.g. departments, groups, teams). The MTO hierarchies control sharing of content (who can see and use what) and the ability to view results and analytics (e.g., the manager is able to view performance results for all their team members). An MTO Group Admin role is defined as a mid-tier role which can support MTO management tasks (e.g., move users around, provide permissions) without needing or having full org admin access.

The Resource Pools available in the Admin section allow org admins and managers to sub-allocate CPU/RAM/licenses at a granular level within the MTO, so that limits can be set on what each department or group of users can consume. Resource consumption can be viewed in the Reports and Analytics section.

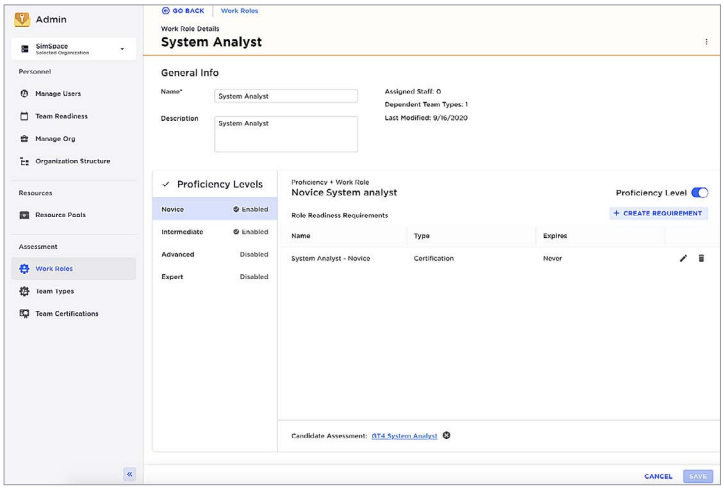


Work Roles

Work Roles define the requirements for a particular position in your organization, such as "System Analyst" or "Network Analyst". Similar to a job description, a Work Role defines what is needed for any user to meet the requirements for that position, such as:

- What pre-existing requirements must be met for that particular position
- What types of certifications are needed for this role
- How long each of those certifications are good for

You can define up to four different proficiency levels for each role, each with its own set of requirements and c ertifications. For example, you can define an intermediate-level System Analyst as requiring a score of 45% on Content Module A, whereas an expert level Analyst must have a score of 75% on that same Content Module in addition to having a score of 66% on Module B.



Team Composition

The Team Types feature lets you define a group of Work Roles that can be treated as a single unit for repeated use within your organizational structure. A Team can be made up of any number of Work Roles of any Proficiency Level and can also be divided into Subteams for more granularity.

Team Types are used to identify the types of groups which exist in your organizational structure. Assigning a Team Type to a group lets you easily see if all members of your team meet readiness qualifications for that Team Type and when any requalifications may be needed.

The organization admin or team manager can define the structure of the team (Work Roles) and assign team members to those roles. The readiness of the team may be defined by the number of team members required per role and whether they meet role readiness requirements.

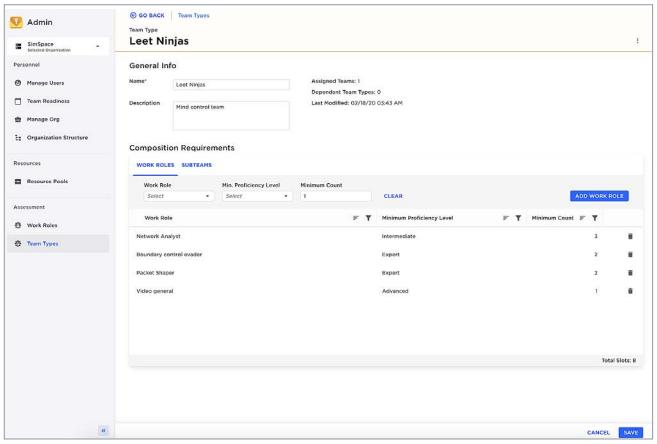
Examples of Team Types are the following:

- **CSIRT: Computer Security Incident** Response Team
  A CSIRT performs three main tasks:
  1. Receives information on a security breach
  2. Analyzes it
  3. Responds to the sender

The CSIRT team may consist of:

- **Team leader:** Directs CSIRT and is responsible for response procedures, including analysis and updates for future incidents
- **Incident leader:** Coordinates individual responses and is an expert on the area/ equipment where the incident occurred
- **Support members:**
  - IT: Expert on overall IT infrastructure
  - Management: Communicates with management regarding concerns from both sides
  - PR: Communicates with public and/or customers to maintain business relationships
  - Legal: Advises on likely ramifications for organization or individual(s) involved

- **SOC: Security Operations Center**
  SOC personnel are responsible for continuously monitoring and analyzing an organization's security arrangements, with the goal of protecting its infrastructure and its data. Analysts and engineers, supported by managers/admins, staff the SOC and oversee day-to-day security operations. They convene CSIRTs (internal or external) for additional support when required. Membership of a SOC will vary from organization to organization, but the following roles will be common in most SOCs:
  - Chief Information Security Officer (CISO): Responsible for defining the overall security operation of the organization; may also manage compliance tasks and communicate with management regarding security issues
  - Manager: Oversees all SOC activities, including managing other members and creating new policies and procedures
  - Security Engineer: Maintains and recommends new monitoring/analysis tools; builds security architecture and liaises with developers to ensure systems are up to date
  - Security Analyst: Detects, investigates, and responds to threats; may also implement additional security measures where required



SimSpace Platform Data Security

Security is a core capability within the platform and extends across multiple areas to ensure that sensitive data is protected from unauthorized users.

Security controls include:

- Online user approvals
- Use of two-factor authentication (2FA) using time-based one-time password (TOTP)
- Use of IP whitelists to limit locations which can access the platform
- User acknowledgement and consent banners
- Platform roles control application access and permissions (e.g., users, managers, admins)
- Multi-tiered management of organizational departments, teams, crews, and users
- Encryption of all data in transmit and at rest
- Single sign-on (SSO) across all applications and services
- Lockout policies to disable accounts after a predefined number of failed login attempts

---

Tech Ops

SimSpace has developed the Tech Ops management application within the SimSpace platform to collect and visualize data from the data center infrastructure (computers, storage, network, VMware) and Cyber Range software. This enables data center and range administrators and operators to monitor, manage, and get insights on how the system is performing and how well it is satisfying users.

Data collected from the Tech Ops management application includes:

- Active users, active ranges, total and available VMs, top users, response times
- Infrastructure data (includes overall CPU and memory loads, disk usage and performance, networking load and performance)
- VMware vCenter performance (includes CPU, memory, tasks, datastores load)
- Help Desk ticket performance and analytics
- Power draw from each of the racks by PDU (assumes network monitoring on the PDUs)
- Performance information on the SimSpace applications
- Performance information on the microservices
- Platform usage and analytics (where users are coming

[17] A PDU (Power Distribution Unit) takes electricity from a main power supply and distributes it to multiple devices.

Support and Collaboration Tools

Chat

- Provides public and private channels (e.g., Blue, Red)
- Provides for private direct message (DM) between participants of same org
- Supports file upload/download from outside and inside the range

Notifications

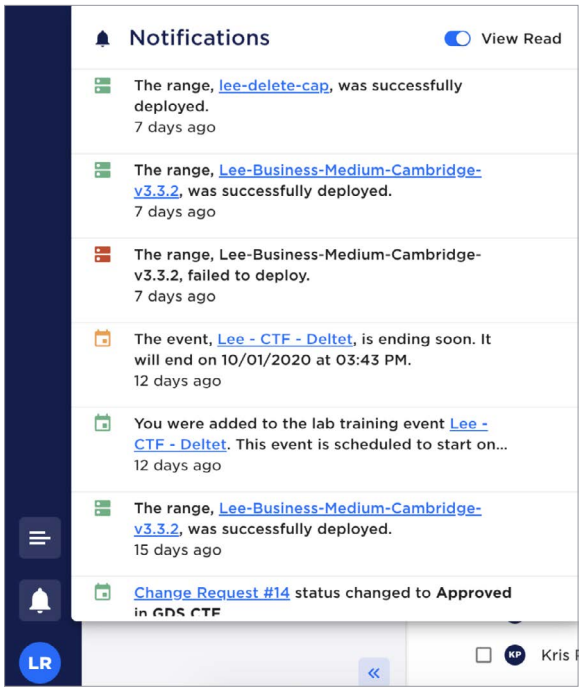
- Platform alerts and notifications
- Deep linking to alerting component
- Example notifications include Build Deployment Completion, Users' event started or RFI status changed

Background Activity Monitor

- Progress update on long-running tasks like OVA puppet module uploads

Help Desk

- Submission of user trouble tickets with status and resolution
- Submissions for new content requests
- Submission of IT requests or security incidents



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.

2022 ©SimSpace Corporation. All rights reserved.