THE SIMSPACE CYBER RANGE

Make complex and laborious network environments simple to create and provide accessible, affordable, and sophisticated solutions to meet your cybersecurity research, development, testing, and training needs.
Required Elements for Network Cloning

Many components must be installed and configured like the real network; fully automated build process
Cyber Range Hosting

Cloud-Based
- Range-as-a-service
- Hosted in public cloud (AWS, Google)
- Isolated environment
- Nearly unlimited capacity
- Rapid updates

SimSpace Hosted
- Range-as-a-service
- Hosted at SimSpace datacenter
- Isolated environment
- Increased data assurances
- Rapid updates
- Inclusion of physical devices

Enterprise
- Hosted on-premises
- Tied into existing infrastructure
- Controlled access, data and results
- Integrate with physical devices
- Integrate with internal systems
Cloud Components & Security

- **User access policies & management**
- **Network access policies**
- **Nested virtualization engine**
- **Software defined networking**
- **DHCP**
- **DNS**

### AWS Foundation Services
- **Compute**
- **Storage**
- **Database**
- **Networking**

### AWS Global Infrastructure
- **Availability Zones**
- **Regions**
- **Edge Locations**

- Centrally manage users, access policies, networks, test/training results and security controls
- High performance nested virtualization and overlay network
- Secure capsule. Isolated self-contained environments – prevent leakage into cloud
Catalog: Preconfigured Networks

Mini-network
- Internet emulation
- Mini network enclave

Size: 15 hosts
Difficulty: -

Generic Small
- Internet emulation
- 1 Simple network
- Red Team hosts

Size: 40 hosts
Difficulty: -

Generic Medium
- Internet emulation
- 4 Simple networks
- Red Team hosts

Size: 80 hosts
Difficulty: 0.91

Military
- Internet emulation
- Island defense
- Tri-service network
- Military critical system

Size: 150 hosts
Difficulty: 1.26

Generic Financial
- Internet emulation
- Financial business units
- Core financial services
- 3rd Party network

Size: 280 hosts
Difficulty: -
RANGE BUILDOUT

Representative Reduction
- Match architecture, operating systems, & applications
- Match security tools and configurations
- Match user and network behavior
- Reduce number of hosts to manageable number
- Select representative lines of business

Step 1
SCOPING

Enterprise Network

Step 2
NETWORK CLONE DEFINITION

Step 3
BUILD

Step 4
TUNE

Setup rules & policies for defensive tools

Custom Built Network

Range Computing Infrastructure

2 weeks | 1 week | 2 weeks | 1 week

SCOPING | NETWORK CLONE DEFINITION | BUILD | TUNE
Cloud-Based Cyber Range

- Creation of new network blueprints: up to 30 mins
- Time to copy blueprint: less than 1 min
- Number of network blueprints and variations (e.g. A/B testing, individual networks per team): nearly unlimited (AWS S3)
- Time to deploy range to computing infrastructure: up to 30 mins
- Range costs: only pay for range use (execution time) not infrastructure or number of copies
- No user scheduling or resource allocation concerns
Generic Financial Network Overlay

Operating Systems
- Windows 2008 R2
- Windows 7
- CentOS, Ubuntu, Kali

Security Tools
- Symantec SEP
- Splunk, Tanium, Qualys
- RSA Netwitness
- Security Onion
- ELK, GRR

Network Instances
- Copies for team training
- Copies for new products (A/B testing)

General
- 280 nodes
- 15 span ports

Applications
- MS Office
- IE, Chrome, Firefox
- Active Directory, Exchange
- IIS, Apache

IT Dept

Branch/Brokerage

Financial Line of Business Network

Financial Line DMZ

Internet

3rd party Techco Inc.

Range

Public DMZ

Data Centers

Financial Line Services

Financial Line of Business Network

ATMs

3rd Party Techco Inc.
Enterprise User Emulation

Traffic generation via intelligent host-based agents to accurately emulate enterprise activity

VIRTUAL USERS
- Unique personas with their own accounts, documents, user behaviors, application biases, social groups, projects
- Interact with real applications on each host (e.g. MS Office, IE, Firefox) like a typical user
- Collaborate with other users to accomplish broader tasks
- Can scale to thousands of users across platform types
- Generate realistic workload on each host & network
- Create means for attackers to exploit clients & hide in enterprise traffic
Attack Tools

Attacks tools to simulate sophisticated attacks, APT1, CyberSnake, etc...

Run attack scenarios automatically by combining discrete attacker tasks to form a full attack.

Custom malware exercising blue’s ability to identify and contain malware communications and persistence utilizing all common techniques.

BREACH: Attack Platform, Reports
OPFOR: Opposing Force, Attacker
WORMHOLE: 0-day attack surrogates
Assessment Tools

**Network Monitoring & MISSION REPLAY**
Visualize traffic flows; replay attacker actions

**Event TRACKING**
Coordinate, record actions from Red & Blue

**Traffic Generation STATUS**
Monitor emulated user activity

**Mission Impact DISPLAY**
Business function dependencies on IT assets
Data Collection and Reporting

Data collected from multiple sources to provide reports, mission impact and scorecards.

Detailed information collected from each emulated user about application and host performance.
Example Uses

**R&D**
On-demand network environments and tools to develop novel cybersecurity solutions

**TESTING**
Assess products across suite of network environments and attack scenarios

**ANALYSIS**
Run the latest malware and attacks for analysis in a safe laboratory environment

**TRAINING**
Team-based training against sophisticated adversaries in a safe and controlled environment

**EXERCISES**
Test your organizational preparedness to withstand sophisticated attacks and disruptive events

**COMPLIANCE**
For regulated industries leverage the network clone for compliance stress testing

**ASSESSMENTS**
Test your tools, people and processes against a suite of attack scenarios to identify areas for improvement

**SALES & POCs**
Showcase product capabilities in a realistic and representative enterprise environment
www.simspace.com

SimSpace

Boston, MA (HQ)
51 Melcher St.
Boston, MA 02210
www.simspace.com

CONTACT US

William Hutchison, CEO
Hutch@simspace.com
Lee Rossey, CTO
Lee@simspace.com
Bart Gray, COO
Bartman@simspace.com

Sales & Business
sales@simspace.com
General Inquiry
contact@simspace.com
Tech Support
support@simspace.com
Example Products Used in the Range

- Any tool that can run in VMWare
- Operating Systems:
  - Windows servers & clients, Ubuntu, Kali
- Applications
  - MS Office, IE, Chrome, Firefox
  - Active Directory, Exchange, IIS, Apache, …
- Security Tools:
  - Symantec SEP, McAfee ePO
  - RSA Netwitness, Tanium, GRR
  - Splunk, Kibana, Snort, Bro, Alien Vault
  - CyberReason, Carbon Black - Bit9
  - Many others …

Example software that can be deployed

| GoogleChrome | flashplayerplugin | git.install | notepadplusplus.install | javaruntime | 7zip.install | adobereader | vlc | dotnet4.5 | vcredist2010 | winpcap | wamp-server | atom | nodejs.install | ccleaner | sysinternals | filezilla | vim | putty.install | libreoffice | mysql.workbench | paint.net | svn | hg | curl | pdfreator | wget | calibre | wareshar | gimp | sourcetree | dotnet3.5 | python2 | cdburnerxp | baretail | foxfinder | firefox | 0ad | microsoftsecurityessentials | audacity | defragger | steam | specy | tor-browser | 1password | jdk7 | nmap | pidgin | googleearth | emacs | cpu-z | innosetup | powergui | ffmpeg | eclipse | make | sudo | awscli | autoit | openoffice | logparser | directorymonitor | popcomtime | spybot | ie11 | mobaxterm | openvpn | redis | autoruns | vmwareplayer | aimp | packer | cyberduck.install | intelligidea-community | binginfo | filezilla.server | bleachbit | xbm | nscp | vmwarevsphereclient | hxd | sharex | btsync | cygwin | malwarebytes | nant | console2 | chromium | windirstat | Tortoisesvn | blender | jenkins | nagios | lastpass | combofix | ultravnc | r.Project | golang | openssl.light | poweriso | clamwin | pycharm-community | webstorm | logmein.client | hittrack.app | Jrt | keepass.install | silverlight | rsat | sqlite |