A Scalable and Comprehensive Security Testing Platform

Security supersedes most, if not all, technical requirements when evaluating, deploying and operating critical infrastructure components. Without security there is no reliability, and with no reliability, how can one be secure?

True security is about finding vulnerabilities and adding patches, compliance, passwords and controls.

Testing Security is about discovering the failure points in your applications, devices, operations and processes. It uses real and reliable traffic, leveraging technology, test and measurement, processes, training and data analytics. Spirent’s security-testing platform provides a scalable and comprehensive solution.

Hyper-realistic simulations

Apps and security traffic generated by CyberSiege can be detected, identified and isolated by firewall engineers, IPS engineers, security analysts and network engineers using Application-level firewalls, IPS, antivirus applications, DDoS appliances, routers, switches, and other networking devices.

CyberSiege provides a vast array of real-world traffic for security testing, including:

- **Social & Internet Apps** that stream real video and audio, including popular properties such as Twitter and Facebook; search engine traffic for Google, Yahoo, and Bing, in addition to web mail and chat services like Gmail, Yahoo Mail, Hotmail, and Yahoo Messenger
- **Mobile Apps** now account for a big chunk of the Internet traffic. Simulate hundreds of mobile Apps, for the most popular mobile devices on Android and iOS clients, to server transactions for multiple user agents and App IDs
- **Enterprise Services** that an IT organization provides to their user base. These services range from email services based on the IMAP, POP and SMTP protocols to database services for MySQL and Oracle databases. Spirent solutions provide testing services based on the SIP protocol which is a fundamental requirement for Cyber Range traffic generators

Testing integration

CyberSiege integrates easily with security devices and Cyber Range environments supporting security device evaluations and bake-offs, and operations training. CyberSiege can physically connect to firewalls, IPS, load balancers, servers, routers and switches.
CyberSiege

CyberSiege is a Next Generation Security Platform (NGSP) that assures security robustness for commercial and government operators, service providers and enterprises.

NGSP should:
- Be comprehensive, scalable and flexible
- Be able to improve the security posture of critical infrastructures, enterprises, applications, and enclaves
- Support assessments, test & measurement, simulations, operations, and training
- Help accelerate the deployment of new infrastructure and services

A scalable NGSP should:
- Feature subscription services and support on-going updates of relevant and zero-day security attacks, malware, Internet Apps, application protocols, enterprise protocols and advanced fuzzing algorithms
- Be able to expand the schema, size and format of its databases and software applications

A flexible NGSP should:
- Have a role in production, staging and test networks
- Support Cyber Range OPS and training
- Be able to facilitate operations training of Incident Response Teams (IRT), firewall engineers, IPS engineers, security analysts and network engineers
- Simulate realistic traffic seen at enterprises, Data Centers, Network Operations Centers (NOC) and Security Operations Centers (SOC/NOSC)

NGSP generate realistic traffic to assess and evaluate critical infrastructure components. Critical infrastructure includes multiple network elements: client and server computing devices, mobile devices, security devices and network devices.
Features

**Simplicity and user-friendly**—Spirent builds the most user-friendly and intuitive User Interfaces (UI) in the industry. You do not have to be a mathematician or scientist to operate CyberSiege.

**IANA traffic selector (select subnet IP addresses by country)**—Test with additional realism and problem solving challenges for training personnel by using more than one IANA network address per country by simply selecting a region on a global map.

**Generate haystack traffic (realistic traffic at scale)**—When testing application-aware devices, it’s critical that the mix reflects real-world conditions from L2 - L7. Create tests that utilize the interactions of real users on real devices as they use real applications for unprecedented realism.

**Generate needle to be found (attacks and malware)**—Quickly generate security attacks that map to Common Vulnerabilities and Exposures (CVE) including malware, signature attacks, and protocol fuzzing. Create custom tests for unique protocols and applications without scripting and leverage smart remediation tools to shorten the time to fix vulnerabilities.

**Generate DDoS Attacks (volumetric to application layer)**—Run line-rate DDoS attacks with legitimate traffic to exercise security devices under real-world conditions. Apply next-generation DDoS attacks to the test cycle with a growing set of L2 - L7 attacks.

**Support multiple networks (enclaves) per port**—Create traffic emulated from multiple networks for the best risk mitigation testing architecture, multiple layers of protection and defense-in-depth can be configured to avoid a single point-of-failure.

**Support virtual routers (to emulate traffic coming from multiple sources)**—Create traffic “from the Cloud.” Test performance, availability, security and scale of OpenStack, VMware vCloud, Cloudstack, Amazon Web Services, and other cloud services.

**REST API (for automation)**—Make your automation environment independent of scripting or programming language, and operating system. Orchestrate with other devices. Automate many other technologies within a test case.
Spirent Services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements.

For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

CyberSiege for effective Cyber Range operations & training

A Cyber Range is a training environment used to train OPS personnel who support operations in network, security, and/or data centers. Its main function is to train on how to defend critical infrastructure assets and launch attacks against simulated critical infrastructure targets in the cyberspace domain. U.S. military classification now defines cyberspace as:

“A global domain within the information environment consisting of the interdependent network of information technology, infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

This domain also includes networks and elements that do not use the TCP/IP protocol such as Industrial Control System (ICS) and Global Navigation Satellite Systems (GNSS.) There are multiple GNSS systems in use today that include the Global Positioning System (GPS), Galileo, GLONASS and BeiDou.

Next Generation Cyber Ranges provide:

Simulation

- Need to present comprehensive simulation and realism of the Internet, including regional and country traffic, emulating real IP addresses using host and network addresses assigned by Internet Assigned Number Authority (IANA.)

Critical infrastructure targeting

- Should be able to load critical infrastructure targets and generate security attacks against them. Traffic generators should be able to import data to rapidly configure the target traffic profiles.

Multimedia realism (including Skype, Voice over IP (VoIP) and Voice over LTE (VoLTE))

- Should emulate voice, video, and audio services that include traffic generators capable of generating real video and audio that can be seen and heard using Internet client applications such as browsers.