

CyberNEXS Global Services

A new cyber training, exercising, competition and certification product for protecting your critical data assets

The Cyber Network EXercise System — CyberNEXS

CyberNEXS helps develop the skills to recognize and defend against cyber attacks. It provides a web-based network management tool that aids in real-time feedback and focused training. CyberNEXS will simultaneously exercise IT staff in an environment that emulates a corporate infrastructure to enhance a real-world training experience.

“Fight as You Train” CyberNEXS Benefits

Live, realistic and available from anywhere in the world, CyberNEXS prepares your security professionals, network administrators, system administrators and students with the tools and skills they need to effectively protect and defend your critical IT systems against today’s real-world threats.

- Trains onsite or remotely against real-world, live cyber threats
- Exercises skills in secure configuration, intrusion detection, incident mitigation and forensics
- Trains in a separate environment similar to that in which the customer operates
- Provides real-time feedback to reinforce and focus training
- Performs automated analysis of the individual and the team
- Trains as a team to baseline the level of knowledge and proficiency
- Uses reconfigurable system architecture to emulate customer environment
- Enables scalability to hundreds of simultaneous Internet-based contestants
- Permits White, Blue and Red Team functions to be performed from any location



The CyberNEXS Team was recently recognized for its contribution to Science, Technology, Engineering and Mathematics (STEM)-related support provided to the Air Force Association (AFA) Cyber Patriot Program and the San Diego Mayor’s Cyber Cup. These important cyber competitions are conducted to encourage high school and middle school students to pursue a career in cybersecurity.



SAIC is a leader in delivering cybersecurity training and exercising and is the competition engine for the Air Force Association (AFA) National High School Cyber Defense Competition.

Why Competition?

Over the last six years, SAIC has been delivering cybersecurity training and exercising to government, Department of Defense, and commercial customers around the world. In every engagement, we have found that the challenge of the competition brings out the best in people. They not only prepare harder to be the best, but they perform follow-up training to discover what they didn't know during the competition.

Essential Cyber Training Phases

CyberNEXS supports four essential training phases:

Instruction – Classroom

- Teaches facts
- Allows questions and answers
- Provides instructor demonstrations

Exercise – Live Lab

- Reinforces learning
- Provides students with hands-on experience
- Enables real-time feedback using trial and error method

Competition – Game

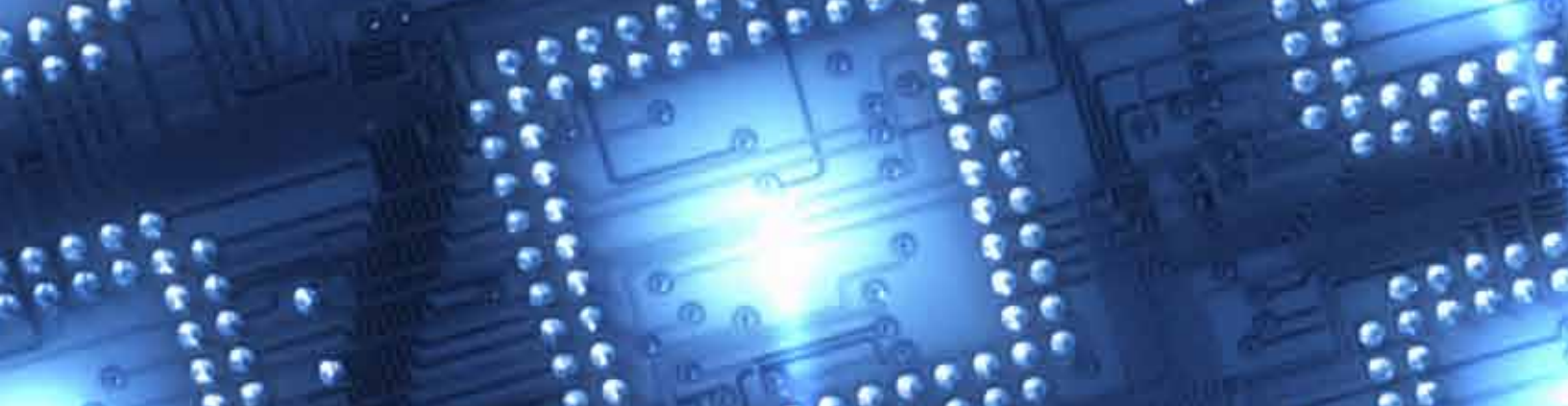
- Measures individual or team
- Enables participants to share knowledge
- It's fun and stimulates contestants to learn more

Certification – Demonstrate Practical Knowledge

- Provides final verification of level of capability
- Certifies contestants while under pressure



SAIC Achievement Award for
Excellence in Community Relations
presented to the CyberNEXS Team



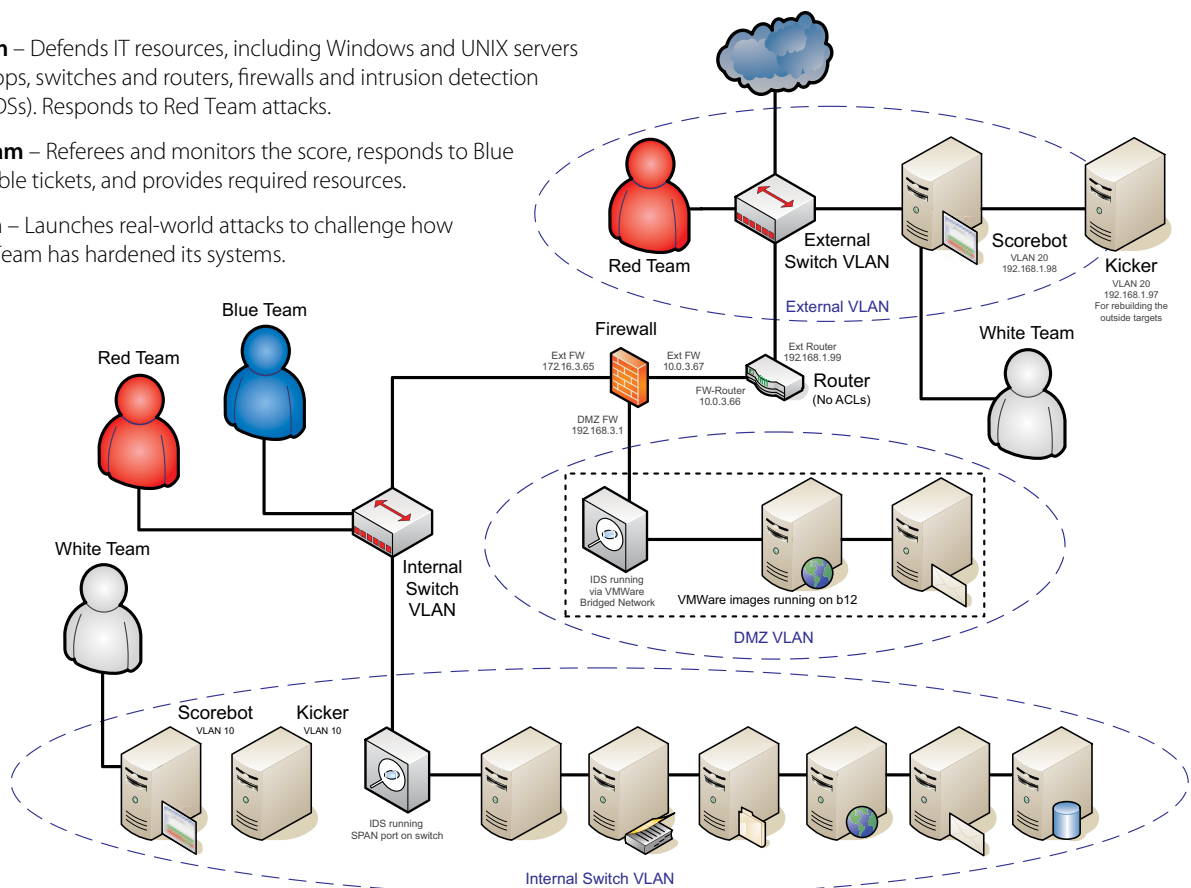
Cybersecurity Training Requirements

The system is self-contained; it never touches the operational environment. It emulates the users' operational environment using standard Windows®, UNIX®, network management interface and network and security devices. It is a realistic, live environment with real-time, automated, quantitative scoring. There is a capability to rerun the same scenario providing the same results. The system is currently available anytime, anywhere, and the complexity of the training can be scaled to the users' level. It is automated for ease of use, and the outbrief capability shows status, trends and scores for rapid feedback.

Blue Team – Defends IT resources, including Windows and UNIX servers and desktops, switches and routers, firewalls and intrusion detection systems (IDSs). Responds to Red Team attacks.

White Team – Referees and monitors the score, responds to Blue Team trouble tickets, and provides required resources.

Red Team – Launches real-world attacks to challenge how well Blue Team has hardened its systems.



Virtual Large Area Network



The CyberNEXS System

The CyberNEXS 1.0 release contains the following components:

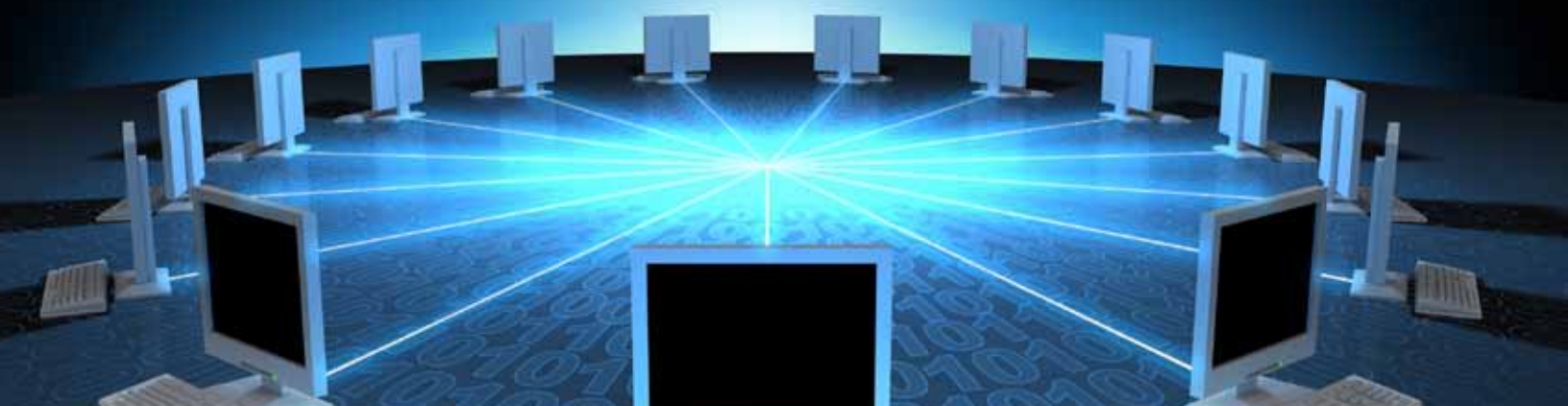
1. CyberNEXS (native client installers for Windows and Linux®)
2. CyberNEXS software (non-native) for Linux (CNG Server, PHP code)
3. Details of needed RPMs for CentOS 5.0 (as in “yum install mysql”)
4. Third-party installers and licenses for needed items (i.e., OpenJMS, JbossWeb)
5. Sample profiles
6. Sample targets
 - CentOS 5 IDS (.68)
 - Windows 2003 Domain Controller (.100)
 - CentOS Mail Server (.101)
 - Windows 2003 Web Server (.102)
 - Windows 2000 Web/SQL Server (.103)
 - Windows XP Desktop (.155)
 - Windows Vista Desktop (.156)
7. CngProxy (non-native) as configured with profiles for router and switch
8. Documentation

Documentation

1. System Overview
2. System Administrator Manual
3. Game Administrator Manual
4. Blue Team User Guide
5. White Team User Guide
6. Red Team User Guide
7. Understanding CyberNEXS Target Profiles



CyberNEXS has been certified by NSA for the System Administration, CNSSI-4013 Advanced Level as part of the SAIC System Administrators Security Training (SAST) curriculum.



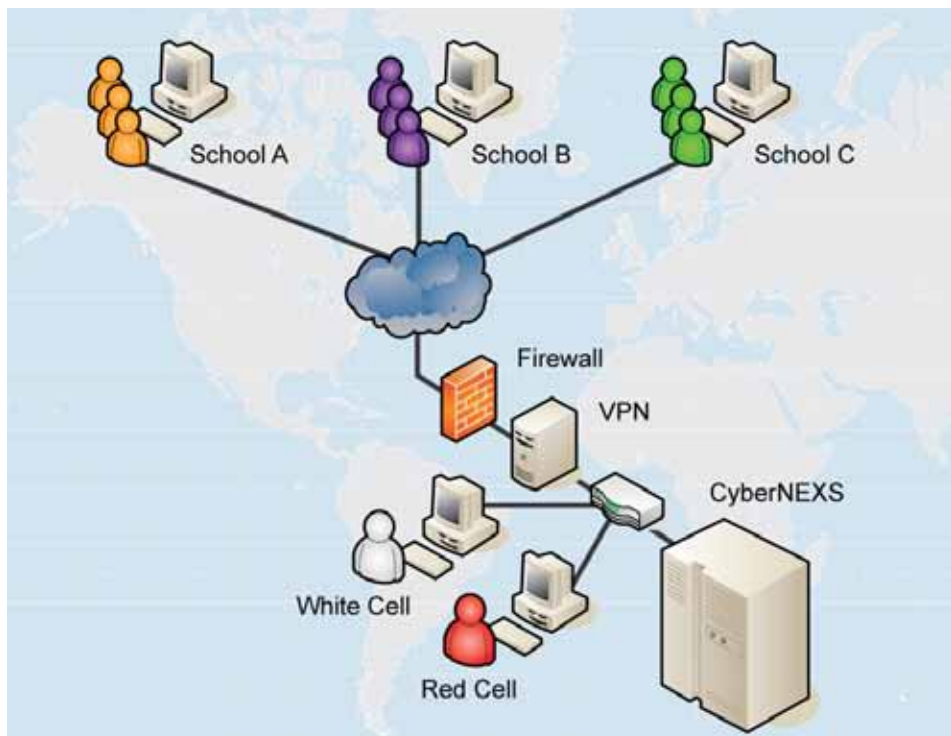
Game Modes

Distributed Game (Practice/Qualification Rounds)

- Contestants download and harden targets on their own machines
- Contestants maintain critical services on their own machines
- Agent sends status to CyberNEXS Global Services, which returns score to contestant's status page
- No attacks or trouble ticket activity performed (no Red or White Team required)

Centralized Game (Final Round)

- Contestants remotely log in to CyberNEXS Global Services
- Hardening, critical services, attacks and trouble ticketing run and scored on CyberNEXS (Red and White Team required)
- Red, White and Blue Teams function local or remote



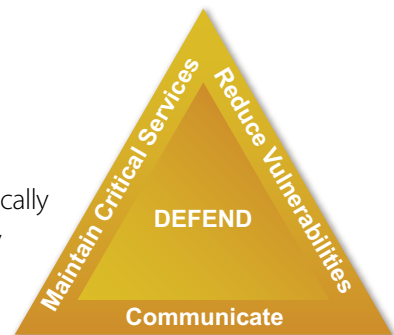
SAIC is dedicated to maintaining the most up-to-date library of target configurations and hacker exploits, as well as continuing to offer a greater variety of training and exercising modules.

Post-Exercise Reconstruction

At the end of the exercise, the instructor can freeze the training environment and walk the students through the various ways their performance was documented and displayed. These charts and graphs depict the status of critical services and vulnerabilities, and the students begin to understand and compare what they did versus what was actually happening. It is through this trial-and-error method that the students apply their knowledge and improve their skills.

Primary Skills

CyberNEXS automatically scores these primary skills on a minute-by-minute basis:



- Maintenance of critical services, even during intrusion and misuse
- Removal of vulnerabilities and hardening systems
- Communicating status and resource requirements
- Thwarting hackers and mitigating their activities



Duke Ayers, VP, Program Manager

tel: 858.826.5150 | email: ayerscar@saic.com

10260 Campus Point Drive | San Diego, CA 92121

Visit us online at: saic.com

saic.com/cybernexs/video.html • saic.com/cybernexs/#media-downloads

Energy | Environment | National Security | Health | Critical Infrastructure



© Science Applications International Corporation. All rights reserved. SAIC, the SAIC logo, and "From Science to Solutions" are trademarks or registered trademarks of Science Applications International Corporation in the United States and/or other countries. CentOS is owned by The CentOS Project. Jboss is a registered trademark of Red Hat, Inc. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. OpenJMS is a product of The OpenJMS Group. UNIX is a registered trademark of x/Open Company in the U.S. and/or other countries. VMware is a registered trademark of VMware, Inc. in the U.S. and/or other countries.