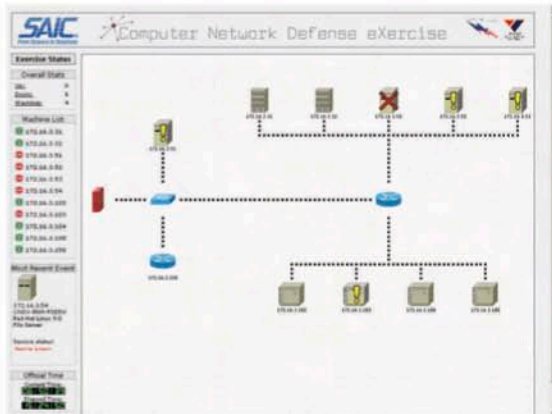
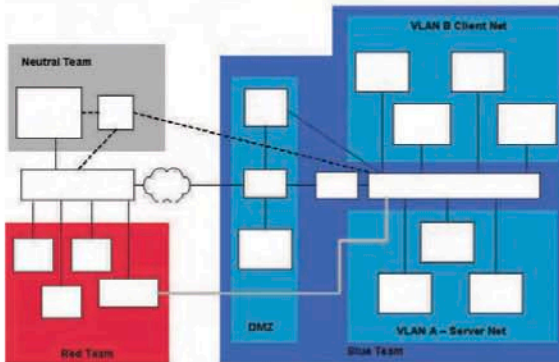


RECOGNIZE AND DEFEND AGAINST CYBER ATTACKS

- **Web-Based Network Management tool aids in real-time feedback and focused training.**



- **Simultaneously exercise your IT staff in an environment that emulates your corporate infrastructure to enhance a real-world training experience.**



A CyberPatriot Initiative



SAIC'S INTELLIGENCE AND INFORMATION SOLUTIONS

TeamDefend

A New Training Model for Defending the Company Network

For more information contact:

Bernt L. Oydna

Science Applications International Corporation
10260 Campus Point Drive
San Diego, CA 92121
858.826.5508
oydnab@saic.com

BSD is a registered trademark of The Regents of the University of California in the United States and/or other countries. CITRIX is a registered trademark of Citrix Systems, Inc. in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds in the United States. Macintosh is a trademark of the Apple Computer, Inc. in the United States and/or other countries. MS Windows is a registered trademark of the Microsoft Corporation in the United States and/or other countries. Novell is a registered trademark of Novell, Inc. in the United States and/or other countries. Plan 9 is a trademark of Lucent Technologies in the United States and/or other countries. QNX is a registered trademark of QNX Software Systems in the United States and/or other countries. SCO is a registered trademark of The SCO Group, Inc. in the United States and/or other countries.

©2007 Science Applications International Corporation. All Rights Reserved.

SAIC
From Science to Solutions

BEYOND NETWORK SECURITY...

“Fight as you Train”

TeamDefend Benefits

- Train to **real-world, live cyber threat**
- **Train on-site; no travel required**
- Exercise skills in **secure configuration, intrusion detection, incident mitigation and forensics**
- **Train in similar, but separate environment** in which the customer operates
- **Real-time feedback system provides current training system status**
- **Self-contained trainer at customer site**
- Automated **analysis of man and machine**
- Technical design permits easy **tailoring of architecture** to match customers' requirements
- **Trains as a TEAM** to baseline the level of knowledge and proficiency

TeamDefend Trains Your IT Staff

- To **identify vulnerabilities** and **lock down systems** (network, server and/or workstation) according to the organization's security policy
- To **configure router policies** according to the organization's security policy
- To **configure and monitor** host-based and network-based intrusion detection systems (ids)
- To **recognize hacker/computer misuse activity**
- To **properly respond** to hacker exploits and computer misuse activity in accordance with company directives
- To **conduct forensics** and collect data For prosecution



SAIC's Cyber Engineering

- Conducted over **450 commercial and government** penetration testing (Pen Test) vulnerability assessments
- **Internal 4-day Pen Test certification** curriculum includes assessment process, code of ethics and use of SAIC exploitation (Red Team) toolkit, as well as hands-on, proficiency demonstration by successfully attacking test targets
- **Up-to-date Pen Test lab** that encompasses over 30 different operating system versions, including MS Windows®, BSD®, Linux®, SCO®, CITRIX®, Macintosh™, Novell®, Plan 9™ and QNX®, as well as routers, switches, firewalls and wireless targets
- **SAIC's proprietary toolkit** includes over 2000 open-source exploits and more than 20 proprietary exploits, all of which have been code-walked for trojans and tested for interoperability; plus other resources
- Initiated **CyberPatriot** to foster routine Cyber Defense training between Academia and State, Federal and Department of Defense organizations
- Participated in **five DefCon Rootwars**
- Conducted the **2003 Toorcon Rootwars Tournament**

...WE HELP DELIVER PEACE OF MIND

saic.com