

VIPER Security Assessment Training

With recent, well-publicized toll fraud and other UC security breaches, there is a significant spike in demand for VoIP/UC Security Assessments. For the first time, VIPER Lab™ (Voice over IP Exploit Research), the UC Security pioneer, is offering VoIP penetration testing training to its partners and customers. Ideal for security assessment professionals and consultants, the assessments performed during training mimic real-world application in a production environment.

After completing this course, participants receive a certificate of completion, and will be able to offer penetration testing to existing and potential customers, adding value to your customer offerings while opening new and profitable revenue opportunities.

VIPER Training Details

The VIPER Security Assessment Training (VAST) is a three-day hands-on training program which provides partners and customers with a systematic method for:

- ▶ Applying VoIP expertise to independently analyze an existing customer network for potential threats and vulnerabilities using security assessment tools.
- ▶ Determining the impact VoIP threats and vulnerabilities could have on a customer network.
- ▶ Recommending corrective action to mitigate potential VoIP threats and vulnerabilities.
- ▶ Positioning VoIP security assessments to prospective customers.

Who should attend?

The VIPER Security Assessment Training is intended for:

- ▶ IT Security Specialists
- ▶ VoIP Security Specialists
- ▶ VoIP Security Engineers
- ▶ Security Assessment Consultants

Or those who wish to apply their VoIP expertise to assess customer networks for potential vulnerabilities, and whose job-related functions might include:

- ▶ Performs system analysis, design, development, test and evaluation activities.
- ▶ Performs vulnerability assessments.
- ▶ Remains current on tools used to identify and potentially exploit vulnerabilities.
- ▶ Works closely with system owners to coordinate testing and clearly articulate issues and assessment findings.
- ▶ Provides expert guidance on mitigation strategies and effective system configurations to alleviate security issues.

Training Specifics

The VIPER Security Assessment Training consists of 14 modules spanning three days and covering the following key knowledge areas:

- ▶ VoIP Fundamentals, VoIP Threats and Vulnerabilities
- ▶ Information Security Principles, Securing VoIP Networks
- ▶ Threat Assessment Methodology, Assessing VoIP Threats, Pen-Testing Methodology
- ▶ Using Threat Assessment and Pen-Testing Tools
- ▶ Ethical Use of Assessment Tools
- ▶ Positioning Threat Assessments and Pen-testing to Customers

The VIPER Security Assessment Training is offered through Instructor-led training at Siper Systems in Richardson, Texas or onsite at your facility.

The VIPER Security Assessment Training includes the following collateral per person:

- ▶ (1) Full color 3 ring binder with printed training modules
- ▶ (1) VIPER Security Assessment Training Workbook
- ▶ (1) VAST (Security Assessment Tools) DVD

Learn from Experts in the field of UC security

Founded by Siper Systems to uncover the vulnerabilities of Unified Communications and VoIP, the VIPER Lab is a state-of-the-art research facility and a team of expert vulnerability assessment professionals. Some of the world's largest and most successful companies rely on the VIPER team to uncover communications risks and vulnerabilities, and improve the security posture of their mission-critical VoIP and UC communications infrastructures.

After completing the VIPER Security Assessment Training, participants will be able to:

- ▶ Describe the basic fundamentals behind VoIP technology and how VoIP is commonly deployed in a customer network.
- ▶ Identify the potential threats and vulnerabilities specific to VoIP networks.
- ▶ Use their understanding of generally accepted information security principles to develop a security posture snapshot of a customer network.

- ▶ Compare VoIP security vendors and identify VoIP specific technologies and best practices used to secure VoIP networks.
- ▶ Employ multiple techniques to assess VoIP related threats in a customer network - including: establishing a fingerprint, Device profiling, Scanning, and Validating scanning results.

Prerequisites:

VoIP Fundamentals, VoIP Threats and Vulnerabilities

- ▶ Exposure to the Linux Operating System or other Unix-based OS.
- ▶ Grasp of the TCP/IP protocols.
- ▶ A minimum of one year experience performing network or application security assessments is strongly recommended.

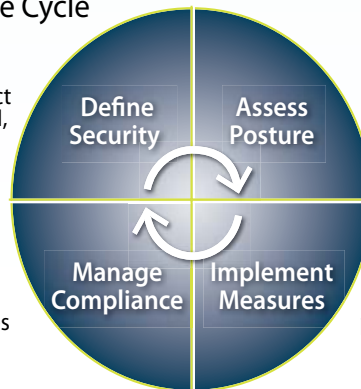
If you are unsure if you meet the required prerequisites, contact us for a quick network security training skill check.

For pricing and scheduling information, please contact a Siper Account Manager or your Siper Reseller.

Unified Communications Security Life Cycle

1. Define Security Requirements
Compare business objectives for UC with impact on information security compliance: HIPAA, PCI, FERPA, GLBA and others

4. Manage Compliance
Review established posture, manage change, gather new requirements as business objectives and regulatory mandates change



2. Assess Security Posture
Identify vulnerabilities, assess risk, determine gap between posture and requirements, consider impact on real-time application performance

3. Implement Security Measures
Optimize security posture and application performance; configure policy enforcement, threat protection, access control, privacy (encryption)

UNIFIED COMMUNICATIONS UNLEASHED

About Siper Systems

Siper Systems, the leader in real-time Unified Communications (UC) security solutions, is the choice of enterprises and service providers around the world to support their mission-critical UC deployments.

Siper offers groundbreaking solutions that secure voice, video, messaging, collaboration, and other real-time communications in converged IP networks, boosting compliance with information security requirements and simplifying the adoption of UC. Siper's innovative *Borderless UC™* architecture delivers secure and private enterprise-class communications to any device over any network in any location.

Backed by the industry-leading research of the VIPER Lab, Siper's award-winning UC-Sec appliance provides comprehensive threat protection, policy enforcement, access control, and encryption in a single, flexible, plug-and-play device. The UC-Sec is pre-integrated with all market-leading UC vendor solutions and is the world's first UC security device to be Common Criteria certified, meeting the stringent international standard for IT security.

V# 03.30.11



SIPERA SYSTEMS
1900 Firman Drive, Suite 600
Richardson, TX 75081, USA

T: +1.214.206.3210
F: +1.214.206.3215
E: info@sipera.com

www.sipera.com