SSL Visibility 4.3 Administration

COURSE DESCRIPTION

The SSL Visibility 4.3 administration course enables you to plan, implement, configure and managed your SSLV appliance(s).

Delivery Method

Instructor-led

Duration

2 days

Course Objectives

By the completion of this course, you will be able to:

- Describe the need for encrypted traffic management (ETM)
- Decide on the best implementation for SSLV in your environment
- Set-up the appliance and configure policies to match your requirements
- Integrate SSLV in an existing PKI
- Maintain SSLV for optimum performance

Who Should Attend

The SSL Visibility 4.3 Administration course is intended for students who wish install and manage the SSLV appliance in a production environment.

Prerequisites

This course assumes that students have a basic understanding of:

- SSL/TSL
- TCP/IP
- Network security devices
- ProxySG

Interactivity

There is no access to a live SSLV appliance. However, the content and activity with provide similar level of familiarity with the solution.

At the end of the course, you will participate in a capture the flag event to test your skills against your classmates. Do you have what it takes to be the best SSL Visibility administrator?

COURSE OUTLINE

Module 1: Removing blind spots by introducing the SSLV

- This first module details the issue of SSL traffic and why it is a blind spot in many networks and what the SSL Visibility appliance can do to resolve this critical issue.

Module 2: Deploying SSLV in your environment

- Deploying the SSLV in your network environment, covering the architecture and flexibility of the SSLV implementation and deployment options. Complete the initial configuration and licensing of the SSLV.

Module 3: SSLV Management and visibility of SSL traffic

- Generating server certificates and disposition of SSL traffic using RSA and Elliptical Curve keys to view encrypted traffic.

Module 4: Removing pain points with SSLV

- Enhancing the capabilities of network security infrastructure while preserving the security of SSL/TLS encryption with SSLV integration.

Module 5: Implementing PKI on the SSLV

- Utilizing PKI functionality, Certificate Authorities and Hardware Security Module options.

Module 6: Maintaining SSLV for optimum service and security

- Using built-in reporting tools to ensure compliance, monitor network and device health status, as well as alerting and log files to diagnose issues. Covering daily tasks and disaster recovery.