SYMANTEC SSL VISIBILITY 4.3 ADMINISTRATION

DURATION: 2 DAYS

COURSE OVERVIEW

The SSL Visibility 4.3 administration course enables you to plan, implement, configure and managed your SSLV appliance(s). This is a lecture-only course, there will be no hands-on access to an SSLV appliance during the course.

There is no access to an SSLV appliance. However, the content and activity will 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?

TARGET AUDIENCE

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

COURSE OBJECTIVES

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

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

COURSE CONTENT

Module 1: Introduction to Encrypted Traffic Management

1. This lesson introduces the pain point introduced by the increasing adoption of SSL/TLS. This lesson also covers the fundamentals about SSL and TLS encrypted communication.

Module 2: Introduction to Encrypted Traffic Management with Symantec SSLV

1. This lesson, introduces the hardware offerings, architecture and capabilities of SSLV.

Module 3: Deploying the SSLV

1. This lesson covers the initial setup phase all SSLV administrators need to accomplish before customizing the configuration to match their requirements. And basic setup to decrypt SSL/TLS in three common installations.

Module 4: Migrate and Upgrade SSLV

1. This lesson covers the procedures to backup and restore an SSLV appliance. This lesson also covers the upgrade process from 4.x and the migration process from 3.x

Module 5: Expose Encrypted Inbound Traffic for Security Devices While Maintaining Security Levels

1. This lesson covers the configuration of SSLV to inspect traffic to servers you manage. It will use passive and active devices and maintain appropriate crypto levels.

Module 6 Expose Encrypted Outbound Traffic for Security Devices and Prevent Data Loss

1. This lesson covers the configuration of SSLV to inspect outbound traffic and use DLP to monitor data loss.

Module 7: Expose Encrypted Threats for Forensic Analysis While Maintaining Compliance Regulations

1. This lesson covers the configuration of SSLV to provide decrypted traffic to a passive device such as Security Analytics while complying with international privacy requirements.

Module 8: Offload SSL Decryption to Improve Proxy SG Efficiency

1. This lesson guides you through the implementation of SSL Decryption offload with one or multiple Proxy SG/ASG to increase throughput for encrypted traffic in your network. Multiple Proxy SG/ASG and SSLV scenarios are implemented here.

Module 9: Simplify Management of multiple SSLV Appliances with Management Center

1. This lesson introduces the capabilities of Management Center with the SSLV to provide visibility, simplified administration and centralized policies.

COURSE PREREQUISITES

This course assumes that students have a basic understanding of:

1. SSL/TSL
2. TCP/IP
3. Network security devices

4. Proxy SG