SYMANTEC SSL VISIBILITY 5.0 ADMINISTRATION

DURATION: 2 DAYS

COURSE OVERVIEW

The SSL Visibility 5.0 Administration course enables you to plan, implement, configure and managed your SSLV virtual appliance. This course includes both lecture and hands-on labs that access the SSLV virtual appliance.

The content and activity in this course will provide solid familiarity with the SSLV solution. At the end of the course, participants will have configured the SSLV in several of the most common implementations to inspect encrypted traffic, sending it to both active and passive security devices.

TARGET AUDIENCE

The SSL Visibility 5.0 Administration course is intended for students who wish install and manage the SSLV virtual 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 virtual 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

- 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 the SSLV Virtual Appliance

- This lesson introduces the new SSLV virtual appliance (SV-VA) and the differences between the virtual appliance and the physical appliances.

Module 3: Introduction to Encrypted Traffic Management with Symantec SSLV

- This lesson introduces the architecture and capabilities of SSLV physical appliance. How the SSLV solves encrypted traffic issues is discussed.

Module 4: Deploying the SSLV

- This lesson covers the architecture and deployment options of the SSLV physical appliance as well the basic setup to decrypt SSL/TLS in three common installations is discussed.

Module 5: Migrate and Upgrade the SSLV

- This lesson covers the migration and upgrade processes and requirements of the physical SSLV appliances.

Module 6: Expose Encrypted Inbound Traffic for Security Devices While Maintaining Security Levels

- 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 7: Expose Encrypted Outbound Traffic for Security Devices and Prevent Data Loss

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

Module 8: Expose Encrypted Threats for Forensic Analysis While Maintaining Compliance Regulations

- 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 9: Offload SSL Decryption to Improve Proxy SG Efficiency

- 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 10: Simplify Management of multiple SSLV Virtual Appliances with Management Center

- 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