Content Analysis 2.x: Administration

COURSE DESCRIPTION

The *Content Analysis 2.x: Administration* course is designed for the network, IT security, and systems administration professionals in a Security Operations position who are tasked with implementing and managing the malware web filtering features of Content Analysis 2.x.

This course covers the administration and configuration tasks required by the solution administrators. The course also shows how Content Analysis 2.x integrates with other Symantec solution to provide a complete anti-malware ecosystem.

Delivery Method
Instructor-led

Duration
Two-days

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

- Implement the Content Analysis 2.x solution in a production environment.
- Configure the multiple anti-malware engines.
- Integrate Content Analysis 2.x.
- Monitor logs for assessing the health of the solution.
- Detect anomalies and prepare the appliance for troubleshooting with the Symantec support team.

Who Should Attend
Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for Content Analysis 2.x

Prerequisites
You must have a working knowledge of networking concepts, including TCP/IP, ICAP, SSL.

You should be familiar with malware detections techniques such as Anti-Virus or reputation analysis.

Hands-On
This course includes practical hands-on exercises and demonstrations that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Introduction

- Course environment
- Lab environment

Install and Implement Content Analysis.

- Initial Content Analysis configuration
- ICAP Overview and configuration
- API Setup
- Performance Profile configuration

Content Analysis Protection Layers.

- Technology Overview
- Preventing known bad files from reaching your environment
- Protect against known threats
- Detecting threats with artificial intelligence
- Detecting emerging threats through a sandboxed execution

Interface Content Analysis with other Symantec Solutions.

- Increase visibility with Symantec Reporter and Management Center
- Increase forensic knowledge with Security Analytics
- Extending mitigation and filtering with Symantec Endpoint Protection

Maintenance and troubleshooting for Content Analysis.

- Monitoring Content Analysis
- Troubleshooting Content Analysis