

Symantec Content Analysis 2.2 Administration

Course Code: 00032375

Course Description

The *Symantec Content Analysis 2.2 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 2.2.

This course covers the administration and configuration tasks required by the solution administrators. The course also shows how Content Analysis 2.2 integrates with other Symantec solution to provide a complete anti-malware ecosystem.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

- Implement the Content Analysis 2.2 solution in a production environment.
- Configure the multiple anti-malware engines.
- Integrate Content Analysis 2.2.
- Monitor logs for assessing the health of the solution.
- Detect anomalies and prepare the appliance for troubleshooting with the Symantec support team.

Hands-On

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

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.

For further information, please contact your regional education team:

Americas.Education@Broadcom.com | APJ.Education@Broadcom.com | EMEA.Education@Broadcom.com

COURSE OUTLINE

Module 1: Introduction

- Course environment
- Lab environment

Module 2: Install and Implement Content Analysis.

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

Module 3: 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

Module 4: 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 Endpoint Protection

Module 5: Maintenance and troubleshooting for Content Analysis.

- Monitoring Content Analysis
- Troubleshooting Content Analysis

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright © 2021 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.