

Symantec CloudSOC Administration R2

Course Code: 00032852

Course Description

The *Symantec CloudSOC R2 Administration* course provides an overview of the CloudSOC service, covering initial setup, deployment options and service configuration. The courseware introduces each topic with an accompanying workflow and is designed for IT professionals wishing to develop their knowledge and skills to manage the Symantec CASB solution.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

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

- Describe the major functions of CloudSOC
- Import Firewall and/or Proxy information to provide granular information on the current behaviours of your end users
- Configure CloudSOC to monitor data at rest and in motion
- Create policies to monitor and control what is uploaded and with whom data is shared
- Describe important integration points with other products within the Symantec Portfolio

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

- A basic understanding of information security concepts

Certification

250-443: Administration of Symantec CloudSOC R2

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 of Symantec CloudSOC

- Benefits and challenges of Cloud Applications
- Problems CloudSOC solves
- CloudSOC tools, information sources, and traffic flows

Module 2: Configuring the Symantec CloudSOC Portal

- Basic Navigation
- Managing Users, Groups, and Access Profiles
- Administrative Actions in the Settings Menu
- Auditing administrative actions
- Configuring Two-Factor Authentication

Module 3: Identifying and Addressing Potential Risks in Cloud Applications

- Cloud applications and their risks
- The Cloud Application Discovery and Safe Adoption Lifecycle
- The CloudSOC Business Readiness Rating
- Importing firewall/proxy logs
- Using Audit data to inform policy in ProxySG

Module 4: Identifying How Data is Used and Shared in Cloud Applications

- Risk of shadow IT and shadow data
- Risk of malware and advanced threats
- Configuring CloudSOC to collect cloud-application log data
- Understanding how CloudSOC monitors data in motion
- Configuring CloudSOC to monitor data in motion

Module 5: Identifying and Remediating Risky Behavior in Cloud Applications

- Identifying and remediating risky behavior in cloud applications: overview
- Understanding and configuring detectors
- Reviewing anomalous or unauthorized user activity
- Creating ThreatScore-based policies
- Protecting data in Cloud Applications
- Understanding the CloudSOC data protection
- Using CloudSOC to control data exposure
- Integrating CloudSOC with Symantec Data Loss Prevention

Module 6: Understanding Reporting Options in CloudSOC and Third-Party Solutions

- Overview of default CloudSOC reporting
- Integrating CloudSOC with SIEM solutions

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.