SYMANTEC CLOUD SOC ADMINISTRATION R2

DURATION: 2 DAYS

COURSE OVERVIEW

The Cloud SOC R2 Administration course provides an overview of the Cloud SOC 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 the knowledge and skills to manage the Symantec CASB solution

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.

TARGET AUDIENCE

This course is intended for students who wish to master the fundamentals of Cloud SOC. It is designed for students who have not taken any previous training courses about Cloud SOC.

COURSE OBJECTIVES

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

1. Describe the major functions of Cloud SOC
2. Import Firewall and/ or Proxy information to provide granular information on the current behaviors of your end users
3. Configure Cloud SOC to monitor data at rest and in motion
4. Create policies to monitor and control what is uploaded and with whom data is shared
5. Describe integration points with other products within the Symantec portfolio

COURSE CONTENT

Introduction to Symantec Cloud SOC

1. Benefits and Challenges of Cloud Applications
2. Problems Cloud SOC Solves
3. Cloud SOC tools, information sources, and traffic flows

Configuring the Symantec Cloud SOC Portal

1. Basic Navigation
2. Managing Users, Groups, and Access Profiles

3. Administrative Actions in the Settings Menu
4. Auditing administrative actions
5. Configuring Two-Factor Authentication

Identifying and Addressing Potential Risks in Cloud Applications

1. Cloud applications and their risks
2. The Cloud Application Discovery and Safe Adoption Lifecycle
3. The Cloud Application Adoption Workflow
4. The Cloud SOC Business Readiness Rating
5. Importing firewall/proxy logs
6. Using Audit data to inform policy in Proxy SG

Identifying How Data is Used and Shared in Cloud Applications

1. Risk of shadow IT and shadow data
2. Risk of malware and advanced threats
3. Configuring Cloud SOC to collect cloud application log data
4. Understanding how Cloud SOC monitors data in motion
5. Configuring Cloud SOC to monitor data in motion

Identifying and Remediating Risky Behavior in Cloud Applications

1. Identifying and remediating risky behavior in cloud applications: overview
2. Understanding and configuring detectors
3. Reviewing anomalous or unauthorized user activity
4. Creating Threat Score-based policies

Protecting data in Cloud Applications

1. Understanding the Cloud SOC data protection workflow
2. Using Cloud SOC to control data exposure
3. Integrating Cloud SOC with Information Centric Encryption (ICE)
4. Integrating Cloud SOC with Symantec DLP

Understanding Reporting Options in Cloud SOC and Third-Party Solutions

1. Overview of default Cloud SOC reporting
2. Integrating Cloud SOC with SIEM solutions

COURSE PREREQUISITES

This course assumes that students have a basic understanding of information security concepts.