# CloudSOC Administration R2

## COURSE DESCRIPTION

The 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 the knowledge and skills to manage the Symantec CASB solution

### Delivery Method
Instructor-led and Virtual Academy

### 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 behaviors 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 integration points with other products within the Symantec portfolio

### Who Should Attend
This course is intended for students who wish to master the fundamentals of CloudSOC. It is designed for students who have not taken any previous training courses about CloudSOC.

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

### 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.

## COURSE OUTLINE

### Introduction to Symantec CloudSOC

- Benefits and Challenges of Cloud Applications
- Problems CloudSOC Solves
- CloudSOC tools, information sources, and traffic flows

### 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

### Identifying and Addressing Potential Risks in Cloud Applications

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

### 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

### 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 workflow
- Using CloudSOC to control data exposure
- Integrating CloudSOC with Information Centric Encryption (ICE)
- Integrating CloudSOC with Symantec DLP

### Understanding Reporting Options in CloudSOC and Third-Party Solutions

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