



# Symantec CloudSOC R1

## COURSE DESCRIPTION

The Symantec CloudSOC R1 course is intended for IT professionals who wish to develop the knowledge and skills to deploy and manage Symantec CASB/s solution, CloudSOC. This course is intended for users who want to apply Symantec CloudSOC's capabilities to control Shadow Data and Shadow IT in cloud applications

### Delivery Method

Instructor-led / Virtual Academy

### Duration

One day

### Course Objectives

### Who Should Attend

This course is intended for technical users responsible for managing Symantec CloudSOC.

### Prerequisites

You must 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

### Lesson 1: Introduction to CloudSOC

- Challenges brought by the migration to the cloud
- CASB market leaders
- Problems solved by CloudSOC
- CASB use cases
- CloudSOC architecture
- CloudSOC integrations

### Lesson 2: Initial Setup

- Connecting a firewall/proxy to Audit
- Connect cloud applications via Securlets
- Configure cloud applications via Gatelets
- Managing Users, Groups, and Access Profiles
- Configure Single Sign On
- Privacy Settings
- Content inspection and threat protection settings
- IP address profiles

- Data archive
- Reach agent installation
- Elastica SpanVA installation
- Advanced settings tech notes

### Lesson 3: Identify and determine business risk of 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
- Compensatory controls
- Implementing the process in Audit

### Lesson 4: Identify how information is being used in cloud applications

- The risk of shadow data
- Document exposure discovery process
- Implementing the process using Securlets

### Lesson 5: Identify and remediate malicious behavior within cloud applications

- Malicious behavior remediation process
- Implementing the process using Detect, Protect, and Investigate

### Lesson 6: Protect documents in cloud applications from exposure

- Cloud application information protection process
- Implementing the process using Securlets, Protect, and Investigate

### Lesson 7: Creating Reports in Dashboard

- Activity dashboard
- Reporting dashboard and widgets

### Hands-On Labs:

We will practice the implementation of the setup and each of the use cases through a series of exercises using CloudSOC.