Certification Program

Administration of Symantec™ Cyber Security Services (July 2015)
Study Guide

The following tables list the Symantec SCS Certification exam objectives for the *Administration of Symantec Cyber Security Services (July 2015)* exam and how these objectives align to the *Cyber Security Services Boot Camp Recordings*.

Recommended courses to prepare for this exam:

- *Symantec Cyber Security Services Boot Camp*

Familiarity with product documentation for Symantec Cyber Security Services:

- MSS Operations Manual
- MSS Pre-Install Questionnaire
- MSS Supported Products List
- MSS Log Collection Platform Reference Guide
- MSS Log Collection Platform Sizing Tool
- MSS Supported Product QuickStart Guide(s) and Configuration Guides
- MSS Secure Webservice API User's Guide
- MSS Portal Users Guide
- MSS Installation Guide for Off-Box Agents
- DeepSight Intelligence Datafeeds Datasheet
- DeepSight Intelligence Fact Sheet
- Splunk-DeepSight App Integration Guide
- Symantec GIN ArcSight Connector QuickStart Guide
- Managed Services Portal Online Help
- Symantec DeepSight Intelligence Datafeeds Resource Guide
- Risk Fabric DeepSight Datasheet
- DeepSIght Intelligence Threat Ratings

Familiarity with Symantec Managed Services Portal (DeepSight and MSS):

- Symantec Managed Services Portal

Recommended Symantec DeepSight Intelligence Modules:

- Lesson 1: DeepSight Early Warning Services Overview
- Lesson 2: Building Technology Lists
- Lesson 3: Creating Alerts
- Lesson 4: Leveraging Alerts and Research
- Lesson 5: Utilizing DataFeeds
- Lesson 6: Creating Custom Reports
- Lesson 7: Managing the Company Profile, Users, and Licenses

Examples of Hands-on Experience (Real World or Virtual):

- Recommended 1-3 months experience working with the Managed Security Services SOC and Log Collection Platform plus Symantec Managed Security Services Portals (Both DeepSight Intelligence portal and MSS Portal), including performing integration projects with DeepSight Application Programming Interface (APIs).
- Describe the components and services of Symantec Managed Security Services and DeepSight
- Manage accounts within the MSS and DS Portals
- Identify and validate installation prerequisites for the Log Collection Platform including Event Agents and Collectors
- Install, configure and validate the components of the Log Collection Platform or Event
- Perform basic configuration of the Log Collection Architecture
- Understand Event Agents and Collectors
- Understand how to work with the Supported Products List (SPL), and PIQ process with the Symantec MSS SOC
- Use tools to access DeepSight Intelligence Datafeed
- Perform basic integration of the DeepSight Data into Databases or create CSV files
- Generate reports using the MSS or DeepSight portals
- Manage licensing for the Symantec MSS or DS Portals
- Utilize the MSS Portal for asset and vulnerability management
- Create and manage Technology Lists within the DeepSight Intelligence Portal
- Understand and demonstrate knowledge of how incidents are created within the MSS Portal through the MSS Services
- Create basic alerts in Deepsight
- Use custom severity rules in the MSS Portal

For more information on the Symantec Certification Program, visit http://go.symantec.com/certification.

EXAM AREA 1

Scoping and Logging Architecture Design

SCS Exam Objectives	Course Topics
Explain the MSS Logging Solution.	MSS Operations Manual MSS LCP Configuration Guide CSS Education Bootcamp
Describe the MSS managed IDS offering and architecture requirements.	MSS Operations Manual CSS Education Bootcamp
Describe the functionality and architecture of the MSS	MSS LCP Configuration Guide CSS Education Bootcamp

SCS Exam Objectives	Course Topics
Log Collection Platform.	
Explain the different types of log transport methods including but not limited to Syslog, API, Database Query, FTP, and On-Device File monitoring.	MSS LCP Configuration Guide MSS Supported Device QuickStart Guides CSS Education Bootcamp
Identify the customer requirements needed for a successful MSS implementation.	MSS Supported Products List MSS Operations Manual CSS Education Bootcamp MSS LCP Configuration Guide

EXAM AREA 2

Symantec CSS Operations, Onboarding Process

SCS Exam Objectives	Course Topics
Describe the MSS Onboarding process, the use of the Log Collection Platform Sizing tool, and the use of the pre-install questionnaire (PIQ).	CSS Education Bootcamp MSS Operations Manual MSS Attributes Guide MSS Pre-Install Questionnaire MSS LCP Sizing Tool
Identify the roles and responsibilities of various MSS Security Operations Center (SOC) teams.	CSS Education Bootcamp MSS Operations Manual
Explain the infrastructure requirements and installation of the Log Collection Platform.	MSS Log Collection Platform CSS Education Bootcamp MSS Installation Guide for Off-Box Agents
Explain how to leverage existing log aggregation technologies as part of the MSS Log Collection Solution (e.g. Splunk).	MSS Log Collection Platform CSS Education Bootcamp MSS Support Device QuickStart Guide

EXAM AREA 3

Symantec CSS Service Offerings

SCS Exam Objectives	Course Topics
Explain the MSS Security monitoring solution.	MSS Operations Manual CSS Education BootCamp
Describe security incident workflow.	MSS Operations Manual

SCS Exam Objectives	Course Topics
	CSS Education BootCamp
Explain the functionality of the Symantec MSS SOC Technology Platform.	MSS Operations Manual CSS Education BootCamp
Describe the MSS Advanced Threat Protection (ATP) and endpoint monitoring services.	MSS Supported Products List CSS Education Bootcamp MSS Operations Manual
Demonstrate an understanding of common incident types published by MSS.	CSS Education Bootcamp MSS Operations Manual

EXAM AREA 4

Symantec DeepSight Intelligence Service Offerings

SCS Exam Objectives	Course Topics
Describe the functionality of the Symantec DeepSight Intelligence.	DeepSight Intelligence Fact Sheet Symantec DeepSight Intelligence Datafeeds Resource Guide CSS Education Bootcamp
Identify and describe the DeepSight Datafeeds.	DeepSight Intelligence Fact Sheet Managed Services Portal Online Help Symantec DeepSight Intelligence Datafeeds Resource Guide CSS Education Bootcamp
Describe the implementation of DeepSight Datafeeds with third party applications.	Splunk-DeepSight App Integration Guide Symantec GIN ArcSight Connector QuickStart Guide Symantec DeepSight Intelligence Datafeeds Resource Guide Risk Fabric DeepSight Datasheet CSS Education Bootcamp
Explain the deployment and integration of DeepSight Datafeeds.	Splunk-DeepSight App Integration Guide Symantec GIN ArcSight Connector QuickStart Guide Symantec DeepSight Intelligence Datafeeds Resource Guide Risk Fabric DeepSight Datasheet CSS Education Bootcamp
Describe the Managed Adversarial Threat Intelligence (MATI) service.	DeepSight Intelligence Fact Sheet Managed Services Portal Online Help Symantec DeepSight Intelligence Datafeeds Resource Guide CSS Education Bootcamp

EXAM AREA 5

Maintenance Tasks (Monitoring, Troubleshooting, Performance Tuning, and Database Management)

SCS Exam Objectives	Course Topics
Describe the various features and functions of the MSS Portal and API.	MSS Portal API Integration Guide MSS Online Help
Describe the various features and functions of the DeepSight Intelligence Portal.	Symantec DeepSight Intelligence Modules DeepSight Intelligence Portal Online Help DeepSight Intelligence Threat Ratings

If you have questions about the Symantec Certification Program, send an email to Global_Exams@symantec.com.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com