symantec. Certification Program

Administration of Symantec™ Cyber Security Services (July 2015)
Exam Objectives

SECTION 1

Scoping and Logging Architecture Design

- Explain the MSS Logging Solution.
- Describe the MSS managed IDS offering and architecture requirements.
- Describe the functionality and architecture of the MSS 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.
- Identify the customer requirements needed for a successful MSS implementation.

SECTION 2

Symantec CSS Operations, Onboarding Process

- Describe the MSS Onboarding process, the use of the Log Collection Platform Sizing tool, and the use of the pre-install questionnaire (PIQ).
- Identify the roles and responsibilities of various MSS Security Operations Center (SOC) teams.
- Explain the infrastructure requirements and installation of the Log Collection Platform.
- Explain how to leverage existing log aggregation technologies as part of the MSS Log Collection Solution (e.g. Splunk).

SECTION 3

Symantec CSS Service Offerings

- Explain the MSS Security monitoring solution.
- Describe security incident workflow.
- Explain the functionality of the Symantec MSS SOC Technology Platform.
- Describe the MSS Advanced Threat Protection (ATP) and endpoint monitoring services.
- Demonstrate an understanding of common incident types published by MSS.

SECTION 4

Symantec DeepSight Intelligence

- Describe the functionality of the Symantec DeepSight Intelligence.
- Identify and describe the DeepSight Datafeeds.
- Describe the implementation of DeepSight Datafeeds with third party applications.
- Explain the deployment and integration of DeepSight Datafeeds.
- Describe the Managed Adversarial Threat Intelligence (MATI) service.

SECTION 5

MSS and DeepSight Portals

- Describe the various features and functions of the MSS Portal and API.
- Describe the various features and functions of the DeepSight Intelligence Portal.

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