250-425: Administration of Symantec Cyber Security Services (May 2016) SCS Exam

Study Guide v. 1.2

Symantec Study Guide Table of Contents

Recommended Preparation Materials

Recommended Course

- Symantec Cyber Security Services Boot Camp
  - Learn Central
  - eLibrary

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

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

- Symantec Managed Services Portal

Product Documentation Referenced in This Exam

- MSS Operations Manual
- MSS Supported Products List
- MSS Log Collection Platform Reference Guide
- MSS Log Collection Platform Sizing Tool
- MSS Supported Product Quick Start Guide(s) and Configuration Guides
- MSS Installation Guide for Off-Box Agents
- DeepSight Intelligence Fact Sheet
- Managed Services Portal Online Help

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
- 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 working 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
- 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

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the 250-425: *Administration of Symantec Cyber Security Services (May 2016)* exam and how these objectives align to the corresponding Symantec courses and some of the referenced documentation.

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

EXAM SECTION 1

Scoping and Logging Architecture Design

Exam Objectives	Topics from CSS Courses and Documentation
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 Log Collection Platform.	MSS LCP Configuration Guide CSS Education Bootcamp
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 Quick Start Guides CSS Education Bootcamp

Exam Objectives	Topics from CSS Courses and Documentation
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 SECTION 2

Symantec CSS Operations, Onboarding Process

Exam Objectives	Topics from CSS Courses and Documentation
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 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 Quick Start Guide

EXAM SECTION 3

Symantec CSS Service Offerings

Exam Objectives	Topics from CSS Courses and Documentation
Explain the MSS Security monitoring solution.	MSS Operations Manual CSS Education Boot Camp
Describe security incident workflow.	MSS Operations Manual CSS Education Boot Camp
Explain the functionality of the Symantec MSS SOC Technology Platform.	MSS Operations Manual CSS Education Boot Camp

Exam Objectives	Topics from CSS Courses and Documentation
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 SECTION 4

Symantec DeepSight Intelligence Service Offerings

Exam Objectives	Topics from CSS Courses and Documentation
Describe the functionality of the Symantec DeepSight Intelligence.	DeepSight Intelligence Fact Sheet CSS Education Bootcamp
Identify and describe the DeepSight Datafeeds.	DeepSight Intelligence Fact Sheet Managed Services Portal Online Help CSS Education Bootcamp
Describe the implementation of DeepSight Datafeeds with third party applications.	CSS Education Bootcamp
Explain the deployment and integration of DeepSight Datafeeds.	CSS Education Bootcamp
Describe the Managed Adversarial Threat Intelligence (MATI) service.	DeepSight Intelligence Fact Sheet Managed Services Portal Online Help CSS Education Bootcamp

EXAM SECTION 5

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

Exam Objectives	Topics from CSS Courses and Documentation
Describe the various features and functions of the MSS Portal and API.	MSS Portal API Integration Guide MSS Online Help

Exam Objectives	Topics from CSS Courses and Documentation
Describe the various features and functions of the DeepSight Intelligence Portal.	Symantec DeepSight Intelligence Modules DeepSight Intelligence Portal Online Help

Sample Exam Questions

1. Which DeepSight Intelligence Datafeed can be used to create a DNS sinkhole?

   a. DeepSight IP Reputation Datafeed
   b. DeepSight Security Content Automation Protocol (SCAP) Vulnerability Datafeed
   c. DeepSight Security Risk Datafeed
   d. DeepSight Domain and URL Reputation Datafeed

2. What happens when an emergency or critical classified incident is validated by a Symantec Managed Security Service Security Analyst?

   a. an email notification is sent to only those contacts who have defined notification settings within the organization and the Security Analyst will call all company contacts
   b. an email notification is sent to all contacts within the organization and the Security Analyst will call all contacts within 30 minutes
   c. an email notification is sent to only those contacts who have defined notification settings and an SMS alert is sent to emergency contacts
   d. an email notification is sent to only those contacts who have defined notification settings within the organization and the Security Analyst will call company contacts defined within the organization's escalation procedure

3. Which is a valid response to a `GetCustomerDataFeedList()` request?

   a. <FeedType > <ID=21 > <Name=IP Reputation CSV Feed > </FeedType >
   b. <Feed=ID:21; Name="IP Reputation CSV Feed" >
   c. <Feed > <ID > 21; Name="IP Reputation CSV Feed" </ID > </Feed >
   d. <FeedType > <ID >21</ID > <Name > IP Reputation CSV Feed </Name > </FeedType>

4. Which Symantec Managed Security Services incident severity is applied when a validated attack or malicious activity is detected posing a moderate to high risk to a customer environment?

    a. Warning
    b. Critical
    c. Emergency
    d. Informational

5. Which two technology types are currently supported by Symantec Managed Security Services? (Select two.)

    a. Intrusion Detection Systems
    b. Firewall Devices
    c. Mobile Endpoint Solutions
    d. Network Management Hosts
    e. Network QoS Applications

6. Symantec Managed Security Services is able to collect all logged traffic from an Intrusion Detection System (IDS).

    What is stored by the Security Operations Center from this IDS log data?

    a. alert and matching portion of the packet
    b. alert only, no packet capture
    c. alert specific full stream (binary) packet capture
    d. full network capture

7. What needs to be completed on the Symantec Managed Security Services Log Collection Platform (LCP) after installing a Collector onto an Event Agent?

    a. select Add Configuration for the Collector through the Collector Management console
    b. configure a Sensor for the Event Agent through the Settings tab in the console
    c. register the Collector on the LCP using the .SIP file found with the Collector
    d. add the Event Agent to the Collector via the Collector Configuration menu

8. A user installs the Event Agent and notes that the Symantec Managed Security Services Log Collection Platform (LCP) refuses the connection.

   What is the cause of this problem?

   a. The Fully Qualified Domain Name is missing from Domain Name Service (DNS).
   b. The Event Agent is missing a Host file.
   c. The Domain Name Service (DNS) IP is missing.
   d. The LCP is missing a Host file.

9. Which application collects events from security products, processes them, and passes them to the Symantec Managed Security Services Event Agent?

   a. Log Collection Platform
   b. Sensor
   c. Collector
   d. Security Device

10. Which two endpoint protection vendors are supported by the Managed Security Services Advanced Threat Protection offering?

   a. Symantec
   b. Kaspersky
   c. McAfee
   d. AVG
   e. PC-Matic

11. What are the primary functions of the Symantec Managed Security Services Log Collection Platform?

   a. to collect, compress, encrypt and transmit all log data to Symantec Managed Security Services
   b. to perform vulnerability scans and send the results to Symantec Managed Security Services
   c. to detect devices as they connect to the network
   d. to collect, compress, encrypt and transmit only filtered data to the Managed Security Services

12. What is the minimum required hardware a customer must use for the installation of the Symantec Managed Security Services Log Collection Platform onto a physical server?

   a. 16 GB RAM, Dual Quad Core Processor and 250GB Hard Disk Drive
   b. 8 GB RAM, Dual Quad Core Processor and 250GB Hard Disk Drive
   c. 4 GB RAM, Quad Core Processor and 250GB Hard Disk Drive
   d. 2 GB RAM, Dual Quad Core Processor and 50GB Hard Disk Drive

13. How many Symantec Managed Security Service Security Operation Centers exist globally?

    a. 5
    b. 4
    c. 3
    d. 6

14. For which technologies does Symantec offer hosted IDS management consoles?

    a. Sourcefire, Cisco, and ISS
    b. McAfee and Trend Micro
    c. Snort and Sourcefire
    d. TippingPoint, Check Point, and Palo Alto

15. A new customer purchases Symantec Managed Security Services and installs the Log Collection Platform (LCP).

    Which ports need to be open for the Security Operations Center to begin setup of the LCP?

    a. TCP - 22 Inbound and 443 Outbound
    b. TCP - 22 Inbound, 443 Outbound, and 514 Bi-Directional
    c. TCP/UDP - 22 Inbound, 443 Outbound, 514 Bi-Directional, 80 Bi-directional, and 2222 Inbound
    d. TCP - 443 Bi-directional, 80 Outbound, and 2222 Inbound

16. A customer wants to stop alerts temporarily; however the customer still wants to receive the stopped alerts when the customer returns.

    What does the customer set in the Symantec DeepSight Intelligence Portal to accomplish this?

    a. set the Vacation Mode Under Alerts and Alerts delivery during Vacation tabs
    b. set the Vacation Mode Under Alerts and All Alerts tabs
    c. set the Vacation Mode Under Alerts and Set Vacation tabs
    d. set the Vacation Mode Under Alerts and My Alerts tabs

17. What is the minimum hardware/VM specification used for a Symantec Log Collection Platform?

    a. 4 CPUs, 4GB RAM, 250GB HDD
    b. 4 CPUs, 8GB RAM, 250GB HDD
    c. 8 CPUs, 4GB RAM, 250GB HDD
    d. 4 CPUs, 8GB RAM, 180GB HDD

18. How often does the Symantec Managed Security Services Log Collection Platform report back to the Security Operations Center, regardless of whether there are queued logs?

    a. every minute
    b. every five minutes
    c. every ten minutes
    d. every fifteen minutes

19. Which technologies does Symantec Managed Security Services recommend to onboard first to maximize time-to-value from the service?

    a. proxies and web application firewalls
    b. endpoints, operating systems, and HIDS
    c. routers, switches, and VPN gateways
    d. firewalls, IDS/IPS, proxies, and endpoints

20. Which log collection method is used to transport Windows Server logs to the Symantec Managed Security Services Log Collection Platform?

    a. Syslog and Windows remote management
    b. FTP and TFTP
    c. SSH encrypted tunnel to each server
    d. TFTP and Windows Center Operations Manager

Answers

1. D
2. D
3. D
4. B
5. A, B
6. A
7. C
8. A
9. C
10. A, C
11. A
12. D
13. D
14. A
15. D
16. C
17. A
18. B
19. D
20. A