symantec. Certification Program

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

## Contents

SAMPLE QUESTIONS ........ 1

ANSWERS ........ 6

## Sample 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-a , 14-a, 15-d , 16-c , 17-a , 18-b, 19-d, 20-a

**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