DUMPSBOSS.

Endpoint Security Complete - Administration R1

Symantec 250-561

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An administrator needs to create a new Report Template that will be used to track firewall activity. Which two (2) report template settings are optional? (Select 2)

A. Output format

B. Generation schedule

C. Email recipients

D. Time frame

E. Size restrictions

ANSWER: A C

QUESTION NO: 2

Which two (2) skill areas are critical to the success of incident Response Teams (Select two)

A. Project Management

B. Incident Management

C. Cyber Intelligence

D. Incident Response

E. Threat Analysis

ANSWER: C D

QUESTION NO: 3

Which communication method is utilized within SES to achieve real-time management?

A. Heartbeat

B. Standard polling

C. Push Notification

D. Long polling

ANSWER: C

QUESTION NO: 4

What does an end-user receive when an administrator utilizes the Invite User feature to distribute the SES client?

A. An email with a link to directly download the SES client

B. An email with a link to a KB article explaining how to install the SES Agent

C. An email with the SES_setup.zip file attached

D. An email with link to register on the ICDm user portal

ANSWER: D

QUESTION NO: 5

An administrator suspects that several computers have become part of a botnet. What should the administrator do to detect botnet activity on the network?

A. Enable the Command and Control Server Firewall

B. Add botnet related signatures to the IPS policy's Audit Signatures list

C. Enable the IPS policy's Show notification on the device setting

D. Set the Antimalware policy's Monitoring Level to 4

ANSWER: A

QUESTION NO: 6

Which report template includes a summary of risk distribution by devices, users, and groups?

A. Device Integrity

B. Threat Distribution

C. Comprehensive

D. Weekly

ANSWER: B

QUESTION NO: 7

Which two (2) options is an administrator able to use to prevent a file from being fasely detected (Select two)

A. Assign the file a SHA-256 cryptographic hash

B. Add the file to a Whitelist policy

C. Reduce the Intensive Protection setting of the Antimalware policy

D. Register the file with Symantec's False Positive database

E. Rename the file

ANSWER: B D

QUESTION NO: 8

Wh.ch Firewall rule components should an administrator configure to block facebook.com use during business hours?

A. Action, Hosts(s), and Schedule

B. Action, Application, and Schedule

C. Host(s), Network Interface, and Network Service

D. Application, Host(s), and Network Service

ANSWER: A

QUESTION NO: 9

Which two (2) scan range options are available to an administrator for locating unmanaged endpoints? (Select two)

A. IP range within network

B. IP range within subnet

C. Entire Network

D. Entire Subnet

E. Subnet Range

ANSWER: A E

QUESTION NO: 10

What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)

A. Increased content update frequency

B. Increased visibility

C. Reduced 3rd party licensing cost

D. Reduced database usage

E. Reduced network usage

ANSWER: C D