Broadcom

250-605

Symantec Endpoint Protection 14.x Admin R2 Technical Specialist

Latest Version: 6.0

Question: 1

When configuring client-server communication, which two configurations impact the responsiveness of SEP clients to administrative actions?
(Choose two)
Response:

A. Client heartbeat interval
B. SEPM domain name resolution
C. Restart time of Windows Defender
D. Push mode versus Pull mode communication

Answer: A,D

Question: 2

How does SEP determine which network behaviors to block using the default Intrusion Prevention Policy?

A. Based on firewall logging history
B. By referencing a list of known attack signatures
C. Using machine learning to profile new applications
D. By analyzing domain trust relationships

Answer: B

Question: 3

Where can certified virus definitions for Symantec Endpoint Protection Manager (SEPM) be manually downloaded?

A. Symantec Endpoint Protection Manager Home Page
B. LiveUpdate Administrator Console
C. Symantec Security Response website
D. Broadcom License Portal

Answer: C

Question: 4

Which feature of SEP allows administrators to block USB storage devices on both Windows and Mac clients?

A. Host Integrity
B. Device Control
C. Application Control
D. SONAR Protection

Answer: B

Question: 5

How does SEDR help security teams distinguish between suspicious and confirmed malicious activity?

A. By comparing incident names to threat intelligence feeds
B. By mapping events to MITRE ATT&CK stages and correlating artifacts
C. By counting the number of firewall blocks triggered per IP
D. By assigning each endpoint to a specific investigation team

Answer: B

Question: 6

Which factor most influences the data retention duration in a SEDR environment?

A. Number of policies deployed
B. Size of the system image
C. Volume of telemetry data generated per endpoint
D. Frequency of LiveUpdate definitions

Answer: C

Question: 7

What are two key settings that can be defined when configuring SEPM notification conditions? (Choose two)

A. Type of event (e.g., Virus found, Policy non-compliance)

B. Hourly billing rate for impacted hosts
C. Action to take (e.g., quarantine file)
D. Method of alert delivery (e.g., email, SNMP trap)

Answer: A,D

Question: 8

Which two configurations must be in place for SEDR to accurately detect and classify threats?
(Choose two)

A. SEP clients must have telemetry and logging enabled
B. SEDR Management Console must be running on HTTPS
C. SEPM must be running in high-availability mode
D. Endpoint Activity Recorder must be configured and active

Answer: A,D

Question: 9

When manually downloading definitions, which two pieces of information are useful for selecting the correct file version?
(Choose two)

A. The build version of the operating system
B. The virus definition sequence number or date
C. The architecture type (32-bit vs 64-bit)
D. The statically named folder associated with a product version

Answer: B,D

Question: 10

Which feature in SEDR enables security teams to improve detection accuracy over time?

A. Scheduled license auditing
B. Environment tuning through rule configuration and noise reduction
C. On-demand SEP policy regeneration
D. MAC address whitelisting

Answer: B

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer