KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **250-605**

Title : Symantec Endpoint Protection 14.x Admin R2 Technical Specialist

Version : DEMO

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

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

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

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

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