250-561 Q&As

Endpoint Security Complete - Administration R1

Pass Symantec 250-561 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/250-561.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec
Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which alert rule category includes events that are generated about the cloud console?

A. Security

B. Diagnostic

C. System

D. Application Activity

Correct Answer: A

QUESTION 2

Which rule types should be at the bottom of the list when an administrator adds device control rules?

A. General "catch all" rules

B. General "brand defined" rules

C. Specific "device type" rules

D. Specific "device model" rules

Correct Answer: D

QUESTION 3

Which report template type should an administrator utilize to create a daily summary of network threats detected?

A. Network Risk Report

B. Blocked Threats Report

C. Intrusion Prevention Report

D. Access Violation Report

Correct Answer: D

QUESTION 4

Which term or expression is utilized when adversaries leverage existing tools in the environment?

A. opportunistic attack

B. script kiddies

C. living off the land

D. file-less attack

Correct Answer: B

QUESTION 5

A user downloads and opens a PDF file with Adobe Acrobat. Unknown to the user, a hidden script in the file begins downloading a RAT.

Which Anti-malware engine recognizes that this behavior is inconsistent with normal Acrobat functionality, blocks the behavior and kills Acrobat?

A. SONAR

B. Sapient

C. IPS

D. Emulator

Correct Answer: B