250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

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

https://www.geekcert.com/250-441.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 section of the ATP console should an ATP Administrator use to evaluate prioritized threats within the environment?

A. Search

B. Action Manager

C. Incident Manager

D. Events

Correct Answer: B

QUESTION 2

Why is it important for an Incident Responder to copy malicious files to the ATP file store or create an image of the infected system during the Recovery phase?

A. To have a copy of the file policy enforcement

B. To test the effectiveness of the current assigned policy settings in the Symantec Endpoint Protection Manager (SEPM)

C. To create custom IPS signatures

D. To document and preserve any pieces of evidence associated with the incident

Correct Answer: B

QUESTION 3

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Correct Answer: A

QUESTION 4

Which final steps should an Incident Responder take before using ATP to rejoin a remediated endpoint to the network, according to Symantec best practices?

A. Run an additional antivirus scan with the latest definitions. If the scan comes back as clean, rejoin the computer to the production network.

B. Run Windows Update to patch the system with the latest service pack. Once the system is up-to-date, rejoin the computer to the production network.

C. Use SymDiag to run a Threat Scan Analysis on the machine. Once the analysis comes back as clean, rejoin the computer to the production network.

D. Upgrade the client to the latest version of SEP. Once the client is upgraded, rejoin the computer to the production network.

Correct Answer: D

QUESTION 5

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Correct Answer: B