# 250-441 <sup>Q&As</sup>

250-441<sup>Q&As</sup>

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.leads4pass.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 action should an Incident Responder take to remediate false positives, according to Symantec best practices?

A. Blacklist

B. Whitelist

C. Delete file

D. Submit file to Cynic

Correct Answer: B

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/
DOCUMENTATION/10000/DOC10899/en_US/satp_security_ops_guide_3.0.5.pdf?
__gda__=1541987119_a3559016c9355c98c2ec53278a8df2a0 (119)

**QUESTION 2**

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as "finding incursions"?

A. Protect

B. Identify

C. Respond

D. Detect

Correct Answer: B

**QUESTION 3**

What is a benefit of using Microsoft SQL as the Symantec Endpoint Protection Manager (SEPM) database in regard to ATP?

A. It allows for Microsoft Incident Responders to assist in remediation

B. ATP can access the database using a log collector on the SEPM host

C. It allows for Symantec Incident Responders to assist in remediation

D. ATP can access the database without any special host system requirements

Correct Answer: D

**QUESTION 4**

Which stage of an Advanced Persistent Threat (APT) attack do attackers map an organization\\'s defenses from the inside?

A. Discovery

B. Capture

C. Exfiltration

D. Incursion

Correct Answer: A

Reference: http://www.whymeridian.com/blog/bid/399610/5-Stages-of-an-Advanced-Persistent-ThreatAttack-on-Your-Network

---

**QUESTION 5**

What is the earliest stage at which a SQL injection occurs during an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Capture

D. Discovery

Correct Answer: B

250-441 PDF Dumps                    250-441 VCE Dumps                    250-441 Practice Test