



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.passapply.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 access credentials does an ATP Administrator need to set up a deployment of ATP: Endpoint, Network, and Email?

- A. Email Security.cloud credentials for email correlation, credentials for the Symantec Endpoint Protection Manager (SEPM) database, and a System Administrator login for the SEPM
- B. Active Directory login to the Symantec Endpoint Protection Manager (SEPM) database, and an Email Security.cloud login with full access
- C. Symantec Endpoint Protection Manager (SEPM) login and ATP: Email login with service permissions
- D. Credentials for the Symantec Endpoint Protection Manager (SEPM) database, and an administrator login for Symantec Messaging Gateway

Correct Answer: C

Reference: <https://support.symantec.com/us/en/article.howto124667.html>

QUESTION 2

What is the role of Synapse within the Advanced Threat Protection (ATP) solution?

- A. Reputation-based security
- B. Event correlation
- C. Network detection component
- D. Detonation/sandbox

Correct Answer: B

Reference: <https://support.symantec.com/us/en/article.info5060.html>

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

How can an Incident Responder generate events for a site that was identified as malicious but has NOT triggered any events or incidents in ATP?

- A. Assign a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).
- B. Run an indicators of compromise (IOC) search in ATP manager.
- C. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that blocks traffic to the domain.
- D. Add the site to a blacklist in ATP manager.

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO126023.html

QUESTION 5

Refer to the exhibit. An Incident Responder wants to see what was detected on a specific day by the IPS engine.

Which item must the responder choose from the drop-down menu?

The screenshot shows the Symantec ATP interface for "Network Traffic: Malicious: July 21". Under "Network Detections:", there is a drop-down menu currently set to "Blacklist". The menu is open, showing the following options: Blacklist (highlighted), Vantage, Insight, Mobile Insight, Cynic, and AntiVirus Engine. Below the menu, the text "0 of 0 Results" is displayed. A table with columns "Host Name", "IP Address", "Detected By", "Source", "File Name", and "Detection Date" is visible, but it is empty. A message "No data available." is shown at the bottom of the table area.

- A. Insight
- B. Cynic
- C. Vantage
- D. Blacklist

Correct Answer: A