# 250-441$^{\text{Q\&As}}$

Administration of Symantec Advanced Threat Protection 3.0

**QUESTION 1**

How does an attacker use a zero-day vulnerability during the Incursion phase?

A. To perform a SQL injection on an internal server

B. To extract sensitive information from the target

C. To perform network discovery on the target

D. To deliver malicious code that breaches the target

Correct Answer: D

Reference: https://www.symantec.com/connect/blogs/guide-zero-day-exploits

**QUESTION 2**

In which scenario would it be beneficial for an organization to eradicate a threat from the environment by deleting it?

A. The Incident Response team is identifying the scope of the infection and is gathering a list of infected systems.

B. The Incident Response team is reviewing detections in the risk logs and assigning a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

C. The Incident Response team completed their analysis of the threat and added it to a blacklist.

D. The Incident Response team is analyzing the file to determine if it is a threat or a false positive.

Correct Answer: C

**QUESTION 3**

An Incident Responder discovers an incident where all systems are infected with a file that has the same name and different hash. As a result, the organism view has multiple entries for the malicious file.

What is causing this issue?

A. This is a polymorphic threat

B. This is a DDoS attack

C. The file has multiple hashes

D. The file is trying to phone home

Correct Answer: A

**QUESTION 4**

An organization is considering an ATP: Endpoint and Network deployment with multiple appliances. Which form factor will be the most effective in terms of performance and costs?

A. Virtual for management, physical for the network scanners and ATP: Endpoint

B. Physical for management and ATP: Endpoint, virtual for the network scanners

C. Virtual for management and ATP: Endpoint, physical for the network scanners

D. Virtual for management, ATP: Endpoint, and the network scanners

Correct Answer: B

**QUESTION 5**

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

A. Network detection component

B. Event correlation

C. Reputation-based security

D. Detonation/sandbox

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO119277.html