

# CERTPARK



## QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,  
High Passing Rate!  
provides update  
free of charge  
in one year!



<https://www.certpark.com>

**Exam** : **250-441**

**Title** : Administration of Symantec  
Advanced Threat Protection  
3.0

**Version** : DEMO

1.What is the second stage of an Advanced Persistent Threat (APT) attack?

- A. Exfiltration
- B. Incursion
- C. Discovery
- D. Capture

**Answer: B**

2.Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an endpoint?

- A. System Lockdown
- B. Intrusion Prevention System
- C. Firewall
- D. SONAR

**Answer: A**

3.An Incident Responder wants to create a timeline for a recent incident using Syslog in addition to ATP for the After Actions Report.

What are two reasons the responder should analyze the information using Syslog? (Choose two.)

- A. To have less raw data to analyze
- B. To evaluate the data, including information from other systems
- C. To access expanded historical data
- D. To determine what policy settings to modify in the Symantec Endpoint Protection Manager (SEPM)
- E. To determine the best cleanup method

**Answer: BE**

4.Which SEP technologies are used by ATP to enforce the blacklisting of files?

- A. Application and Device Control
- B. SONAR and Bloodhound
- C. System Lockdown and Download Insight
- D. Intrusion Prevention and Browser Intrusion Prevention

**Answer: C**

**Explanation:**

Reference: [https://support.symantec.com/en\\_US/article.HOWTO101774.html](https://support.symantec.com/en_US/article.HOWTO101774.html)

5.What is the role of Insight within the Advanced Threat Protection (ATP) solution?

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

**Answer: A**

**Explanation:**

Reference: <https://www.symantec.com/content/dam/symantec/docs/brochures/atp-brochure-en.pdf>