



# Symantec

## 250-441 Exam

### Symantec Administration of Symantec Advanced Threat Protection 3.0 Exam

Thank you for Downloading 250-441 exam PDF Demo

You can Buy Latest 250-441 Full Version Download

<https://www.certkillers.net/Exam/250-441>

<https://www.certkillers.net>

## Version: 8.0

---

### Question: 1

---

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

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

---

**Answer: B**

---

---

### Question: 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**

---

---

### Question: 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**

---



---

**Question: 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**

---

Reference:

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

---

**Question: 5**

---

DRAG DROP

Which level of privilege corresponds to each ATP account type?  
Match the correct account type to the corresponding privileges.

**Account**

**Privilege**

User

Can add to blacklist

Administrator

Can view incidents

Controller

Can configure Synapse

---

**Answer:**

---

## Privilege

Controller	Can add to blacklist
User	Can view incidents
Administrator	Can configure Synapse

---

### Question: 6

---

What are two policy requirements for using the Isolate and Rejoin features in ATP? (Choose two.)

- A. Add a Quarantine firewall policy for non-compliant and non-remediated computers.
- B. Add a Quarantine LiveUpdate policy for non-compliant and non-remediated computers.
- C. Add and assign an Application and Device Control policy in the Symantec Endpoint Protection Manager (SEPM).
- D. Add and assign a Host Integrity policy in the Symantec Endpoint Protection Manager (SEPM).
- E. Add a Quarantine Antivirus and Antispyware policy for non-compliant and non-remediated computers.

---

**Answer: AD**

---

Reference:

[https://support.symantec.com/en\\_US/article.HOWTO128427](https://support.symantec.com/en_US/article.HOWTO128427)

---

### Question: 7

---

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

---

**Answer: B**

---

---

**Question: 8**

---

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

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

---

**Answer: B**

---

---

**Question: 9**

---

Why is it important for an Incident Responder to analyze an incident during the Recovery phase?

- A. To determine the best plan of action for cleaning up the infection
- B. To isolate infected computers on the network and remediate the threat
- C. To gather threat artifacts and review the malicious code in a sandbox environment
- D. To access the current security plan, adjust where needed, and provide reference materials in the event of a similar incident

---

**Answer: D**

---

---

**Question: 10**

---

Which two database attributes are needed to create a Microsoft SQL SEP database connection? (Choose two.)

- A. Database version
- B. Database IP address
- C. Database domain name
- D. Database hostname
- E. Database name

---

**Answer: BD**

---

## Thank You for trying 250-441 PDF Demo

To Buy Latest 250-441 Full Version Download visit link below

<https://www.certkillers.net/Exam/250-441>

## Start Your 250-441 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your 250-441 preparation with actual exam questions.

<https://www.certkillers.net>