Symantec™ | Certification Program

# 250-441: Administration of Symantec Advanced Threat Protection 3.0 SCS Exam

Study Guide v. 1.0

## Symantec Study Guide Table of Contents

# Recommended Preparation Materials

## Recommended Courses

*http://go.symantec.com/elibrary*

- Symantec Advanced Threat Protection 3.0: Incident Response

## Product Documentation Referenced in This Exam

- Advanced Threat Protection Platform Technical Support articles and alerts: https://support.symantec.com/en_US/advanced-threat-protection-platform.html
- Endpoint Protection Technical Support articles and alerts: https://support.symantec.com/en_US/endpoint-protection.54619.html
- Symantec Advanced Threat Protection Platform 3.0 Installation Guide https://support.symantec.com/en_US/article.DOC10684.html
- Symantec Advanced Threat Protection Platform 3.0 Administration Guide https://support.symantec.com/en_US/article.DOC10683.html
- Symantec Advanced Threat Protection Platform 3.0 Release Notes https://support.symantec.com/en_US/article.DOC10685.html
- Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide https://support.symantec.com/en_US/article.DOC10686.html

## Examples of Hands-on Experience (Real World or Lab)

- Recommended 3-6 months experience working with Symantec Advanced Threat Protection 3.0 in a lab or production environment
- Architecting and integrating Symantec ATP in an environment
- Verifying installation prerequisites for enterprise deployment scenarios
- Performing initial installation and configuration of Symantec ATP
- Configuring and managing components of Symantec ATP
- Managing users and user roles
- Completing audits and reports
- Searching for indicators of compromise (IOC).
- Detecting, investigating, remediating, and recovering from an incident
- Recovering from an outbreak using Symantec best practices

# Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the *Symantec Advanced Threat Protection 3.0* exam and how these objectives align to the corresponding Symantec courses and the referenced documentation.

For more information on the Symantec Certification Program, visit http://go.symantec.com/certification

## EXAM SECTION 1: Cybersecurity Overview

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Describe advanced persistent threats (APTs), including components and examples of these threats | • Advanced Threat Protection 3.0: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA)<br>• Responding to Zero Day Threats – whitepaper |
| Describe the stages of an attack | • Advanced Threat Protection 3.0: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA)<br>• Advanced Persistent Threats: A Symantec Perspective – whitepaper |
| Describe the best practices for protecting your organization | • Advanced Threat Protection 3.0: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA)<br>• Responding to Zero Day Threats – whitepaper |

## EXAM SECTION 2: Advanced Threat Protection Overview

| Exam Objectives | **Topics from**<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Describe the use cases for each of the components that make up the ATP platform | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |
| Given a scenario, determine the appropriate architecture and sizing for an ATP installation | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Determine where to go to collect the information needed (e.g., Dashboard, Incident Manager, Settings) | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Describe the three account types in ATP | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |
| Describe the prerequisites for ATP Email, Endpoint, and Network | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Given a scenario, determine the appropriate global setting configurations | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |
| Describe the types of information that you can find in the Dashboard | • Advanced Threat Protection 3.0: Incident Response - Introducing Advanced Threat Protection (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |

**EXAM SECTION 3: Advanced Threat Protection Endpoint Configuration**

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Determine how to configure Symantec Endpoint Protection (SEP) to communicate with ATP | • Symantec Endpoint Protection 14.0 RU1 Installation and Administration Guide<br>• Advanced Threat Protection 3.0: Incident Response - Optimizing your ATP Environment (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |
| Determine the appropriate configuration settings for ATP and SEP Detection and Response | • Symantec Endpoint Protection 14.0 RU1 Installation and Administration Guide<br>• Advanced Threat Protection 3.0: Incident Response - Optimizing your ATP Environment (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |

### EXAM SECTION 4: Identifying Indicators of Compromise (IOCs)

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Given a scenario, determine the appropriate steps to take to successfully search for IOCs | • Advanced Threat Protection 3.0: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Describe the various types of events that ATP detects | • Advanced Threat Protection 3.0: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Given an incident, analyze the incident and determine next steps | • Advanced Threat Protection 3.0: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Describe the different types of IOC searches | • Advanced Threat Protection 3.0: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help |
| Determine where in the Dashboard to go to view recent activity/incidents | • Advanced Threat Protection 3.0: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |

## EXAM SECTION 5: Responding to Threats

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Determine how to isolate breached endpoints | • Advanced Threat Protection 3.0: Incident Response - Remediating and Isolating Threats (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help<br>• Setting up Host Integrity – Support article<br>• Creating a Quarantine policy for a failed Host Integrity check – Support article<br>• Symantec Endpoint Protection 14.0 RU1 Installation and Administration Guide |
| Determine which action to take in order to remediate malicious files | • Advanced Threat Protection 3.0: Incident Response - Remediating and Isolating Threats (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help<br>• Virus removal and troubleshooting on a network – Support article |
| Describe the process for manually submitting files to Cynic for analysis | • Advanced Threat Protection 3.0: Incident Response - Remediating and Isolating Threats (ILT/VA)<br>• Remediating malicious files and reducing false positives<br>• Advanced Threat Protection 3.0 Help |
| Describe the ATP communication processes | • Advanced Threat Protection 3.0: Incident Response - Preparing your Endpoint Environment for Incident Response (ILT/VA)<br>• Advanced Threat Protection 3.0: Incident Response - Remediating and Isolating Threats (ILT/VA)<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Advanced Threat Protection 3.0 Help |

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Given a scenario, determine how to blacklist suspicious domains, URLs, and IP addresses | • Advanced Threat Protection 3.0: Incident Response - Remediating and Isolating Threats (ILT/VA)<br>• Responding to threats by blacklisting suspicious addresses<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help<br>• Symantec Endpoint Protection 14.0 RU1 Installation and Administration Guide |

## EXAM SECTION 6: Recovering from an Incident

| Exam Objectives | Topics from<br>*ATP 3.0 Documentation and Courses* |
|---|---|
| Describe the best practices for recovering from an incident | • Advanced Threat Protection 3.0: Incident Response - Recovering After an Incident (ILT/VA)<br>• Recovery best practices<br>• Symantec Advanced Threat Protection Platform 3.0 Administration Guide<br>• Symantec Advanced Threat Protection Platform 3.0 Security Operations Guide<br>• Advanced Threat Protection 3.0 Help<br>• Incident Handlers Handbook (SANS Institute) - Whitepaper<br>• Virus removal and troubleshooting on a network – Support article |
| Given a scenario, describe how to create an After Actions Report (AAR) | • Advanced Threat Protection 3.0: Incident Response - Recovering After an Incident (ILT/VA)<br>• Gathering information for reporting<br>• Creating a Lessons Learned report<br>• Guidelines for Evidence Collection and Archiving (IETF) |

**Sample Exam Questions**

1. What is the minimum number of CPU cores required for a virtual ATP Manager in a production environment?

A. 8
B. 12
C. 24
D. 48

2. What is the minimum Internet Explorer version required for accessing the ATP Manager?

A. 9
B. 10
C. 11
D. 12

3. Which option is a valid Database Entity Search Filter for the "Endpoint State" filter type?

A. Good
B. Bad
C. Unknown
D. Active

4. What is the SSH port for connecting to a deployed ATP appliance?

A. 20
B. 21
C. 22
D. 23

5. What is the protocol that ATP: Email scans?

A. FTP
B. SMTP
C. MAPI
C. POP

6. What Advanced Threat Protection technology can retrieve information concerning "load point changes?"

A. Endpoint Data Recorder
B. SONAR
C. Skeptic
D. Vantage

7. What is the maximum number of events per endpoint that can be retrieved conducting a search?

   A. 50
   B. 100
   C. 150
   D. 200

8. 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

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

   A. Submit file to the Cynic
   B. Whitelist
   C. Blacklist
   D. Delete file

10. An Incident Responder added a file's MD5 hash to the blacklist.

    Which component of SEP enforces the blacklist?

    A. System Lockdown
    B. Bloodhound
    C. Intrusion Prevention
    D. SONAR

**Answers:**
1. B
2. C
3. D
4. C
5. B
6. A
7. B
8. A
9. B
10. A