Symantec™ | Certification Program

250-427: Administration of Symantec

Advanced Threat Protection 2.0.2 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 2.x: Incident Response (ILT/VA)
    - Strengthening your Cybersecurity Framework
    - Introducing Advanced Threat Protection
    - Optimizing your ATP Environment
    - Analyzing Events and Incidents for Indicators of Compromise
    - Preparing your Endpoint Environment for Incident Response
    - Remediating and Isolating Threats
    - Recovering After an Incident

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 2.0 Installation Guide
- Symantec Advanced Threat Protection Platform 2.0 Administration Guide
- Symantec Advanced Threat Protection Platform 2.0 Release Notes
- Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide

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

- Recommended 3-6 months experience working with Symantec Advanced Threat Protection 2.x 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 Section Weightings

Section	Weight
Cybersecurity Overview	11%
Advanced Threat Protection Overview	26%
Advanced Threat Protection Endpoint Configuration	16%
Identifying Indicators of Compromise (IOCs)	19%
Responding to Threats	21%
Recovering from an Incident	7%
Total	**100%**

Note: The section weightings represent the percentage of the total item bank dedicated to each section. For more detailed information about each objective found within the sections, review the Exam Objectives section below.

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the *Advanced Threat Protection 2.0.2* exam and how these objectives align to the corresponding Symantec courses and some of 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 *ATP 2.x Documentation and Courses*
Describe advanced persistent threats (APTs), including components and examples of these threats	• Advanced Threat Protection 2.x: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA) ○ Describing advanced persistent threats • Responding to Zero Day Threats – whitepaper
Describe the stages of an attack	• Advanced Threat Protection 2.x: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA) ○ Describing the stages of an attack • Advanced Persistent Threats: A Symantec Perspective - whitepaper
Describe the best practices for protecting your organization	• Advanced Threat Protection 2.x: Incident Response - Strengthening your Cybersecurity Framework (ILT/VA) ○ Describing preventative steps • Framework for Improving Critical Infrastructure Cybersecurity – NIST PDF • Symantec Security Best Practices - Stopping malware and other threats – webpage

EXAM SECTION 2: Advanced Threat Protection Overview

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Describe the use cases for each of the components that make up the ATP platform	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Introducing Advanced Threat Protection
Given a scenario, determine the appropriate architecture and sizing for an ATP installation	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Examining ATP architecture and sizing • Symantec Advanced Threat Protection Platform 2.0 Installation Guide
Determine where to go to collect the information needed (e.g., Dashboard, Incident Manager, Settings, Events, Action Manager)	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Becoming familiar with Symantec ATP • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help
Describe the three account types in ATP	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Creating ATP accounts • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Advanced Threat Protection 2.0 Help
Describe the prerequisites for ATP Email, Endpoint, and Network	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Introducing Advanced Threat Protection • Symantec Advanced Threat Protection Platform 2.0 Installation Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide
Given a scenario, determine the appropriate global setting configurations	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Becoming familiar with Symantec ATP • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Advanced Threat Protection 2.0 Help

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Describe the types of information that you can find in the Dashboard	• Advanced Threat Protection 2.x: Incident Response - Introducing Advanced Threat Protection (ILT/VA) ○ Becoming familiar with Symantec ATP • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Advanced Threat Protection 2.0 Help

EXAM SECTION 3: Advanced Threat Protection Endpoint Configuration

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Describe how to configure Host Integrity and Quarantine Firewall policies for ATP Quarantine	• Advanced Threat Protection 2.x: Incident Response - Optimizing your ATP Environment (ILT/VA) ○ Preparing for Symantec Endpoint Protection integration • Symantec Endpoint Protection 12.1.6 Installation and Administration Guide

Determine how to configure Symantec Endpoint Protection (SEP) to communicate with ATP	• Advanced Threat Protection 2.x: Incident Response - Optimizing your ATP Environment (ILT/VA)
	  ○ Configuring Symantec Endpoint Protection database correlation
	  ○ Configuring the SEPM controller for EDR
	  ○ Configuring ATP as proxy server
	• Symantec Advanced Threat Protection Platform 2.0 Administration Guide
	• Advanced Threat Protection 2.0 Help
	• Symantec Endpoint Protection 12.1.6 Installation and Administration Guide

Determine the appropriate configuration settings for ATP and SEP Detection and Response	• Advanced Threat Protection 2.x: Incident Response - Optimizing your ATP Environment (ILT/VA)
	  ○ Configuring Symantec Endpoint Protection database correlation
	  ○ Configuring the SEPM controller for EDR
	  ○ Configuring ATP as proxy server
	• Symantec Advanced Threat Protection Platform 2.0 Administration Guide
	• Advanced Threat Protection 2.0 Help
	• Symantec Endpoint Protection 12.1.6 Installation and Administration Guide

EXAM SECTION 4: Identifying Indicators of Compromise (IOCs)

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Given a scenario, determine the appropriate steps to take to successfully search for IOCs	• Advanced Threat Protection 2.x: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA) ○ Searching for indicators of compromise (IOC) • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help
Describe the various types of events that ATP detects	• Advanced Threat Protection 2.x: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA) ○ ATP detection overview • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help
Given an incident, analyze the incident and determine next steps	• Advanced Threat Protection 2.x: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA) ○ Analyzing incidents • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help
Describe the different types of IOC searches	• Advanced Threat Protection 2.x: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA) ○ Searching for indicators of compromise (IOCs) • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Determine where in the Dashboard to go to view recent activity/incidents	• Advanced Threat Protection 2.x: Incident Response - Analyzing Events and Incidents for Indicators of Compromise (ILT/VA) ○ Analyzing the Dashboard • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Advanced Threat Protection 2.0 Help

EXAM SECTION 5: Responding to Threats

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Determine how to isolate breached endpoints	• Advanced Threat Protection 2.x: Incident Response - Preparing your Endpoint Environment for Incident Response (ILT/VA) • Advanced Threat Protection 2.x: Incident Response - Remediating and Isolating Threats (ILT/VA) ○ Isolating breached endpoints • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help • Setting up Host Integrity – Support article • Creating a Quarantine policy for a failed Host Integrity check – Support article • How to change the installed feature set on Endpoint Protection 12.1.x clients – Support article • Symantec Endpoint Protection 12.1.6 Installation and Administration Guide

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Determine which action to take in order to remediate malicious files	• Advanced Threat Protection 2.x: Incident Response - Preparing your Endpoint Environment for Incident Response (ILT/VA) • Advanced Threat Protection 2.x: Incident Response - Remediating and Isolating Threats (ILT/VA) ○ Remediating malicious files and reducing false positives • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help • Virus removal and troubleshooting on a network – Support article • Symantec Endpoint Protection 12.1.6 Installation and Administration Guide
Describe the process for manually submitting files to Cynic for analysis	• Advanced Threat Protection 2.x: Incident Response - Remediating and Isolating Threats (ILT/VA) ○ Remediating malicious files and reducing false positives • Advanced Threat Protection 2.0 Help
Describe the ATP communication processes	• Advanced Threat Protection 2.x: Incident Response - Preparing your Endpoint Environment for Incident Response (ILT/VA) • Advanced Threat Protection 2.x: Incident Response - Remediating and Isolating Threats (ILT/VA) • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Advanced Threat Protection 2.0 Help
Given a scenario, determine how to blacklist suspicious domains, URLs, and IP addresses	• Advanced Threat Protection 2.x: Incident Response - Remediating and Isolating Threats (ILT/VA) ○ Responding to threats by blacklisting suspicious addresses • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help • Symantec Endpoint Protection 12.1.6 Installation and Administration Guide

EXAM SECTION 6: Recovering from an Incident

Exam Objectives	Topics from *ATP 2.x Documentation and Courses*
Describe the best practices for recovering from an incident	• Advanced Threat Protection 2.x: Incident Response - Recovering After an Incident (ILT/VA) ○ Recovery best practices • Symantec Advanced Threat Protection Platform 2.0 Administration Guide • Symantec Advanced Threat Protection Platform 2.0 Security Operations Guide • Advanced Threat Protection 2.0 Help • Incident Handlers Handbook (SANS Institute) - Whitepaper • Virus removal and troubleshooting on a network – Support article

Given a scenario, describe how to create an After Actions Report (AAR)	• Advanced Threat Protection 2.x: Incident Response - Recovering After an Incident (ILT/VA)
	  ○ Gathering information for reporting
	  ○ Creating a Lessons Learned report
	• Guidelines for Evidence Collection and Archiving (IETF)

Sample Exam Questions

1. Which threat is an example of an Advanced Persistent Threat (APT)?

    a. CryptoLocker
    b. Flasback
    c. Hydraq
    d. Nimda

2. What is the first stage of an Advanced Persistent Threat (APT) attack?

    a. Incursion
    b. Discovery
    c. Capture
    d. Exfiltration

3. Which cybersecurity function is defined as “understanding where the important data is”?

    a. Identify
    b. Protect
    c. Detect
    d. Respond

4. Which ATP component best detects a phishing attack?

    a. ATP: Email
    b. ATP: Network
    c. ATP: Endpoint
    d. ATP: Roaming

5. An organization has six (6) locations and wants to implement ATP: Network. Each location has between 1,500 and 2,000 endpoints.

    What is the minimum number of appliances needed?

    a. 1 ATP manager, 6 ATP: Network scanners
    b. 6 ATP: Network scanners
    c. 6 ATP managers, 6 ATP: Network scanners
    d. 6 ATP managers, 1 ATP: Network scanner

6. Which section of the ATP console should an ATP Administrator use to see a visual depiction of ATP activity across modules?

    a. Dashboard
    b. Events
    c. Incident Manager
    d. Action Manager

7. Which domain will be blocked by the default SEP Quarantine Firewall policy?

    a. *.symantecliveupdate.com
    b. *.symantec.com
    c. *.norton.com
    d. *windowsupdate.com

8. How does ATP use SSL with Endpoint Detection and Response?

    a. ATP uses the SSL connection when submitting files to Cynic and VirusTotal
    b. ATP uses the SSL connection to ensure secure communication between ATP and Email Security.cloud using trusted certificates
    c. ATP uses the SSL connection to encrypt connection to the Symantec Endpoint Protection Manager (SEPM) SQL database
    d. ATP uses the SSL connection to ensure secure communication between ATP and the Symantec Endpoint Protection Manger (SEPM) using trusted certificates.

9. An Incident Responder is using a STIX file to search for indicators of compromise (IOCs).

    What is the maximum STIX file size that the responder can upload?

    a. 5 MB
    b. 10 MB
    c. 15 MB
    d. 20 MB

10. What kind of information is sent to Symantec when Data Handling is set to “Allow Symantec to use evaluated binaries for generating signatures”?

    a. Types of endpoints on the network
    b. Hashes from discovered financial reports
    c. Fully qualified domain names of computers
    d. Hashes from discovered malware

Answers:

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

Contributors and Subject Matter Experts:

- Shelly Calhoun
- Chris Diya
- Jeremy Dundon
- Jonathan Fencik
- Amanda Grady
- Matthew Kane
- Patrick Martin
- Steven Savill
- Chloe Pinteaux-Jones
- Sr. Principal Technical Education Consultant*

* Some contributors prefer to remain anonymous for privacy reasons so we have listed only their title.