Symantec. Certification Program

250-551: Administration of Symantec Endpoint Detection and Response 4.1

Exam Study Guide v1.0

Exam Description

Candidates can validate technical knowledge and competency by becoming a Symantec Certified Specialist (SCS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored SCS exam that is based on a combination of Symantec training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Symantec Endpoint Detection and Response (SEDR) product in a Security Operations role. This certification exam tests the candidate's knowledge on how to detect, investigate, remediate, and recover from an incident using Symantec Endpoint Detection and Response in their organizations.

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience with Symantec EDR solutions (On Prem and/or Cloud) with at least the ability to complete the following:

- Operational knowledge of Symantec Endpoint Detection and Response.
- Familiarity with Cybersecurity and Threat Protection concepts
- Familiarity with Symantec Endpoint Protection products.
- Perform initial Symantec EDR setup steps.
- Perform basic Symantec EDR Cloud administration actions.
- Configure Symantec EDR to share data with third-party applications.
- Create Blacklist and Whitelist policies.
- Able to investigate threats in the environment.
- Able to act on threats in the environment.
- Able to recover after threats have been contained.
- Able to report on threats in the environment.

Study References

Instructor Led https://www.symantec.com/services/education-services/training-courses

Symantec Endpoint Detection and Response 4.1 Administration **(2 Day Classroom/Virtual)**

- **Introduction to Symantec EDR**
  - Challenges of Threat Hunting with Endpoint Detection (EDR) in the environment
  - How Symantec Endpoint Detection and Response meets User Stories
- **Increasing the Visibility of Suspicious and Malicious Activity**
  - Identifying Evidence of Suspicious & Malicious Activity (Lecture/Lab)
  - Searching for Indicators of Compromise (Lecture/Lab)
- **Decreasing Security Risk by Responding to Security Threats**
  - Isolating Threats in The Environment (Lecture/Lab)
  - Blocking Threats in The Environment (Lecture/Lab)
  - Removing Threats in The Environment (Lecture/Lab)
- **Collecting and Analyzing Forensic Data for the Investigation of Security Incidents**
  - Collecting Forensic Information (Lecture/Lab)
  - Analyzing Forensic Information (Lecture/Lab)

Self-Paced

https://www.symantec.com/services/education-services/elibrary

Symantec EDR 4.1 Administration eLearning

- **Introduction to Symantec EDR**
- **Increasing the Visibility of Suspicious and Malicious Activity**
- **Decreasing Security Risk by Responding to Security Threats**
- **Collecting and Analyzing Forensic Data for the Investigation of Security Incidents**

* This self-paced course provides the student with a high-level overview of the content contained in the instructor led version of the Symantec EDR 4.1 Administration Instructor-Led course and is only recommended for exam candidates that have experience with Symantec EDR.

Documentation

https://support.symantec.com/

Symantec EDR 4.1 Sizing and Scalability Guide	DOC11378
Symantec EDR 4.1 Installation Guide	DOC11360
Symantec EDR 4.1 Administration Guide	DOC11358
Symantec EDR 4.1 Security Operations Guide	DOC11359
Symantec Threat Discovery Guide	DOC11273
Symantec EDR 4.1 Search Fields Reference	DOC11361

Community

- Symantec Connect EDR Community
- Symantec Connect EDR Cloud Community
- Symantec EDR Landing Page
- Symantec EDR Cloud Help

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the ***Symantec EDR 4.1*** exam and how these objectives align to the corresponding Symantec course topics and their associated lab exercises as well as the referenced product documentation. Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

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

EXAM SECTION 1: Symantec EDR and the Evolving Threat Landscape

Exam Objectives	Topics from *Courses/Documentation*
Describe the capabilities and functions of Symantec EDR.	**Symantec EDR 4.1 Administration Course** • Evolving Threat Landscape • *Introduction* **Documentation:** • Symantec EDR 4.1 Administration Guide

Exam Objectives	Topics from *Courses/Documentation*
Describe the challenges faced when threat hunting in the environment and their resultant business objectives.	**Symantec EDR 4.1 Administration Course** • Evolving Threat Landscape • *Introduction* • *Challenges of Endpoint Detection & Response in the environment* **Documentation:** • Symantec Threat Discovery Guide
Describe how Symantec EDR meets business objectives.	**Symantec EDR 4.1 Administration Course** • Evolving Threat Landscape • *Introduction* • *How Symantec Endpoint Detection and Response meets objectives* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide

EXAM SECTION 2: Increasing the Visibility of Suspicious and Malicious Activity

Exam Objectives	Topics from *Courses/Documentation*
Describe the benefits and outcomes of increasing the visibility of suspicious and malicious activity in the environment.	**Symantec EDR 4.1 Administration Course** • Evolving Threat Landscape • *How Symantec Endpoint Detection and Response meets objectives* • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* **Documentation:** • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide
Describe how SEDR increases the visibility of suspicious and malicious activity in a typical environment.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide

Exam Objectives	**Topics from** *Courses/Documentation*
Describe the various types of suspicious and malicious activity found in a typical environment.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Identifying evidence of suspicious & malicious activity* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec Threat Discovery Guide
Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Identifying evidence of suspicious & malicious activity* **Documentation:** • Symantec EDR 4.1 Installation Guide • Symantec EDR 4.1 Administration Guide
Describe the methods used to identify evidence of suspicious and malicious activity.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Identifying evidence of suspicious & malicious activity* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide
Describe the methods used to enable automated security incident notifications with SEDR.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Identifying evidence of suspicious & malicious activity* **Documentation:** • Symantec EDR 4.1 Administration Guide
Describe the various types of Indicators of Compromise (IoC) found in a typical environment.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Searching for Indicators of Compromise* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec Threat Discovery Guide

Exam Objectives	**Topics from** *Courses/Documentation*
Describe installation prerequisites, minimum solution configuration and installation procedures required before identifying IOCs.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Searching for Indicators of Compromise* **Documentation:** • Symantec EDR 4.1 Sizing and Scalability Guide • Symantec EDR 4.1 Installation Guide • Symantec EDR 4.1 Administration Guide
Describe the methods used to search for IOCs using SEDR.	**Symantec EDR 4.1 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Searching for Indicators of Compromise* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec EDR 4.1 Search Fields Reference

EXAM SECTION 3: Decreasing Security Risk by Responding to Threats

Exam Objectives	**Topics from** *Courses/Documentation*
Describe the benefits of reducing security risks by responding to threats in the environment.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec Threat Discovery Guide
Describe the methods SEDR uses to respond to threats in a typical environment.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction* **Documentation:** • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide

Exam Objectives	Topics from *Courses/Documentation*
Describe the various methods used to isolate threats in a typical environment.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction* • *Isolating Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide
Describe installation prerequisites, minimum solution configuration and installation procedures required to isolate threats.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Isolating Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Sizing and Scalability Guide • Symantec EDR 4.1 Installation Guide • Symantec EDR 4.1 Administration Guide
Given a scenario, determine the appropriate method for isolating threats to reduce security risk.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Isolating Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide • Symantec EDR 4.1 Search Fields Reference
Describe the various methods used to block threats in a typical environment.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide
Describe installation prerequisites, minimum solution configuration and installation procedures required to block threats.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec Threat Discovery Guide

Exam Objectives	**Topics from** *Courses/Documentation*
Given a scenario, determine the appropriate method for blocking threats to reduce security risk.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide
Describe the various methods used to remove threats in a typical environment.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction* • *Removing Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Administration Guide
Describe installation prerequisites, minimum solution configuration and installation procedures required to remove threats.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Removing Threats in the Environment* **Documentation:** • Symantec EDR 4.1 Sizing and Scalability Guide • Symantec EDR 4.1 Installation Guide • Symantec EDR 4.1 Administration Guide
Given a scenario, determine the appropriate method for removing threats to reduce security risk.	**Symantec EDR 4.1 Administration Course** • Decreasing Security Risk by Responding to Threats • *Removing Threats in the Environment* • **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide

EXAM SECTION 4: Collecting and Reporting Forensic Data

Exam Objectives	**Topics from** *Courses/Documentation*
Describe the benefits of collecting and reviewing forensic information.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Introduction* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide

Exam Objectives	**Topics from** ***Courses/Documentation***
Describe how SEDR can be used to collect and review forensic information for further investigation of security incidents.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Introduction* • *Collecting Forensic Information* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec EDR 4.1 Search Fields Reference
Describe the various forms of information collected by SEDR in a typical environment.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Introduction* • *Collecting Forensic Information* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide • Symantec EDR 4.1 Search Fields Reference
Describe installation prerequisites, minimum solution configuration and installation procedures required to collect forensic data.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Collecting Forensic Information* **Documentation:** • Symantec EDR 4.1 Sizing and Scalability Guide • Symantec EDR 4.1 Installation Guide • Symantec EDR 4.1 Administration Guide
Given a scenario, determine the appropriate method for the collection of forensic data using SEDR.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Collecting Forensic Information* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide
Describe the methods used to create post incident reports and the benefits to forensic analysis it provides.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Introduction* • *Reporting Forensic Information* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide

Exam Objectives	Topics from *Courses/Documentation*
Given a scenario, determine the appropriate method to create a post incident report using SEDR.	**Symantec EDR 4.1 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Reporting Forensic Information* **Documentation:** • Symantec EDR 4.1 Administration Guide • Symantec EDR 4.1 Security Operations Guide

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. What component consists of cross-platform applications that collect artifacts from endpoints and sends them to SEDR Cloud?

A. Collection Service Agent
B. Dissolvable Server Agent
C. SEDR Scan Agent
D. Cloud Service Agent

2. Which statement relates to the challenges faced from Incomplete Endpoint Remediation?

E. Limited granularity in normal activity
F. Reduced ability to detect advanced attack methods
G. Reduction of orchestration across controls
H. Attack objects remain on endpoint

3. What, in addition to Techniques, does the MITRE Att&ck Matrix consists of?

A. Entities
B. Problems
C. Tactics
D. Solutions

4. What is applied to the Collected Data within SEDR Cloud Tasks?

A. Investigation Playbook
B. Collection Service Agent
C. Dissolvable Agent Server
D. Scan Policy

5. What does a Ranged query do?

A. Returns or excludes data matching the exact field names and their values
B. Returns or excludes data falling between two specified values of a given field
C. Returns or excludes data matching a regular expression
D. Returns or excludes data based on specific values for a given field

6. What is the first step in the SEDR Insight proxy process?

A. SEDR checks to see if the file is blacklisted or whitelisted
B. SEDR returns reputation information
C. The Endpoint sends a reputation lookup to SEDR
D. Symantec Insight replies with reputation information to SEDR

7. Which Cybersecurity function would “deleting a file” fall under?

A. Identify
B. Protect
C. Respond
D. Recover

8. Which Symantec Endpoint Protection (SEP) function is used when isolating a breached endpoint from the SEDR Manager?

A. Quarantine Firewall policy
B. Application and Device Control Policy
C. LiveUpdate policy
D. Centralized Exceptions Policy

9. Which feature of Symantec Endpoint Detection and Response allows for a Process Dump?

A. Synapse
B. Cynic
C. Endpoint Activity Recorder
D. Endpoint Communications Channel

10. What does a medium priority incident indicate?

A. The incident can safely be ignored
B. The incident can result in a business outage
C. The incident does not affect critical business operation
D. The incident may have an impact on the business

Sample Exam Answers:

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