BROADCOM®
SOFTWARE

Exam Study Guide

Exam 250-552: Symantec Security Analytics 8.0 Technical Specialist

Exam Description

Candidates can validate technical knowledge and competency by becoming a Broadcom Technical Specialist (BTS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored BTS 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 Security Analytics product in a Security Operations role. This certification exam tests the candidate's knowledge on how to how to install, configure and administer Symantec Security Analytics.

For more information about Broadcom Software's certification program, see

https://www.broadcom.com/support/education/software/certification/all-exams

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with the Symantec Security Analytics products in a production or lab environment and intermediate networking and security understanding.

Study References

Courses

Symantec Security Analytics 8 Administration (3-Day Instructor-Led or 1.25 hrs hours Self-Paced)

Documentation

Security Analytics Technical Support articles, documentation sets, and alerts including, but not limited to:

- Security Analytics Documentation:
  - Security Analytics 8 Documentation Portal
    https://support.symantec.com/us/en/documentation.1145515.2121507.html
  - Guide for Security Analytics 8.0.x
    https://support.symantec.com/us/en/article.DOC11207.html
  - Install Guides for Security Analytics Virtual Appliance
    https://support.symantec.com/us/en/documentation.1145515.2121507.html
  - Required Ports, Protocols, and Services for Symantec Enterprise Security Products
    https://support.symantec.com/us/en/article.DOC11287.html
  - Tap Placement and Capture Optimization Best Practices for Security Analytics
    https://support.symantec.com/us/en/article.DOC11215.html
  - Best Searching Practices in Security Analytics 8.0.x
    https://support.symantec.com/us/en/article.DOC11214.html
- Training Courses:
  - https://www.symantec.com/services/education-services/training-courses
- Datasheets and White papers
  - https://www.symantec.com/products/network-forensics-security-analytics#resources

Website

- Security Analytics Landing Page
- https://support.broadcom.com/web/ecx/productdetails?productName=Security%20Analytics

Exam Objectives

The following tables list the Broadcom Software SCS Certification exam objectives for the exam and how these objectives align to the corresponding Symantec course topics and their associated lab exercises as well as the referenced product documentation.

It is strongly recommended that all candidates complete all applicable lab exercises in preparation for the exam.

Exam Objectives	Applicable Course Content

Describe how Security Analytics provides visibility by capturing network traffic as it traverses the network	**Symantec Security Analytics 8 Administration**
	• Module: 1, 2, 6, 7
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide

Exam Objectives	Applicable Course Content

Describe the core architecture of Security Analytics, including virtual and hardware appliances	**Symantec Security Analytics 8 Administration**
	• Module: 1, 4
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Install Guides for Security Analytics Virtual Appliance

Exam Objectives	Applicable Course Content

Describe the Symantec Security Analytics network architecture requirements, including the differences between network TAPs and SPAN ports	**Symantec Security Analytics 8 Administration**
	• Module: 1, 4
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Install Guides for Security Analytics Virtual Appliance
	  ○ Tap Placement and Capture Optimization Best Practices for Security Analytic

Exam Objectives	Applicable Course Content

Describe how to configure Security Analytics deployment, including key options within both the CLI and web interface	**Symantec Security Analytics 8 Administration**
	• Module: 1, 4
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Install Guides for Security Analytics Virtual Appliance

Exam Objectives	Applicable Course Content

Describe how to perform basic and advanced filtering, creating indicators, and recommended filtering best practices	**Symantec Security Analytics 8 Administration**
	• Module: 5
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Best Searching Practices in Security Analytics 8.0.x

Exam Objectives	Applicable Course Content

Describe the file extraction process, the resulting artifacts and what they purpose they serve	**Symantec Security Analytics 8 Administration**
	• Module: 6, 7
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Best Searching Practices in Security Analytics 8.0.x

Exam Objectives	Applicable Course Content

Describe the anatomy of a cyber-attack, the steps of the Cyber Kill Chain, and what makes up an Indicator of Compromise (IoC)	**Symantec Security Analytics 8 Administration**
	• Module: 5, 6, 7
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide

Exam Objectives	Applicable Course Content

Describe threat hunting and incident response frameworks and procedures	**Symantec Security Analytics 8 Administration**
	• Module: 2, 3
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide

Exam Objectives	Applicable Course Content

Describe how to create, use, and distribute reports in Security Analytics	**Symantec Security Analytics 8 Administration**
	• Module: 1, 8
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student Guide
	  ○ Best Searching Practices in Security Analytics 8.0.x

Exam Objectives	Applicable Course Content

Describe how Security Analytics integrates with both Symantec and third-party security products	**Symantec Security Analytics 8 Administration**
	• Module: 9
	• Documentation:
	  ○ Guide for Security Analytics 8.0.x
	  ○ Security Analytics 8 Administration Student 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 is the number of storage volumes on a minimal Security Analytics installation?** A. 1 B. 3 C. 4 D. 5
2.	**Which two (2) components of a filter statement will generate autocomplete suggestions, when utilizing the filter bar? (Select two.)** A. Presets B. Elements C. Operators D. Wildcards E. Eliminators
3.	**What does the recycle count refer to in the disk-storage information?** A. The number of slots that have had to be re-indexed B. The number of times the disk volume has been reformatted C. The number of times the disk volume has been manually flushed D. The number of times the capture process has filled the volume and started over
4.	**Which two-factor authentication provider is supported by Security Analytics?** A. OKTA B. RSA SecureID C. Symantec VIP D. Google Authenticator
5.	**Which two (2) of the data types listed can be imported to make an indicator? (Select two.)** A. AJAX B. XML C. JSON D. VBScript E. Java
6.	**What are the maximum number of sensors supported by a single Central Manager Console?** A. 100 B. 25 C. 250 D. 200

7.	**What format are indicators exported in?** A. JSON B. XML C. HTML D. NodeJS
8.	**Which process initiates a TCP session?** A. IP state machine B. Three-way handshake C. Protocol exchange D. Network flow
9.	**Indicators are created in a standardized format that allows for threat intel sharing. What is the language called?** A. OVAL B. CVSS C. STIX D. CybOX
10.	**Why is it recommended to limit the number of widgets on a dashboard?** A. To avoid information overload B. To reduce load on the appliance C. To reduce load on the network D. To avoid large timespans

Sample Exam Answers	
1.	A
2.	B, C
3.	D
4.	D
5.	B, C
6.	D
7.	A
8.	B
9.	C
10.	B