BROADCOM®
SOFTWARE

Exam Study Guide

Exam 250-443: Symantec CloudSOC - R2 Technical Specialist

Exam Description

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

This exam targets IT Professionals using the CloudSOC product in a Security Operations role. This certification exam tests the candidate’s knowledge on how to configure and administer Symantec CloudSOC.

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 CloudSOC in a production or lab environment.

Study References

Courses

Symantec CloudSOC Administration R2

(2 Day Instructor-Led with hands-on labs, or 8-Hour Self-Paced)

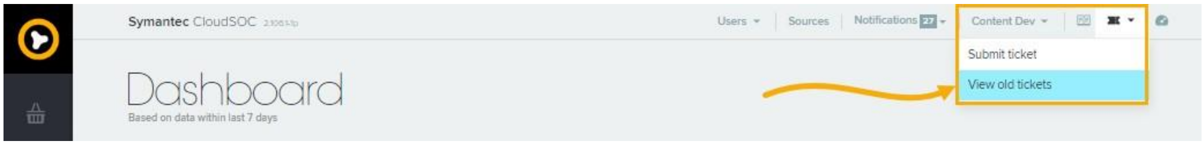
- Configuring the Symantec CloudSOC Portal
- Identifying and Addressing Potential Risks in Cloud Applications
- Identifying How Data is Used and Shared in Cloud Applications
- Identifying and Remediating Risky Behavior in Cloud Applications
- Protecting Data in Cloud Applications
- Understanding Reporting Options in CloudSOC and Third-Party Solutions

Symantec CloudSOC Technical Updates

(eLearning)

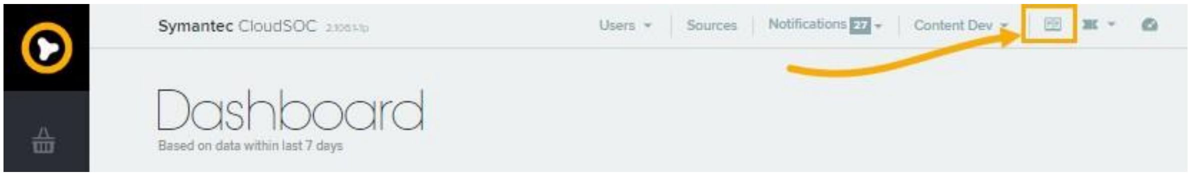
Documentation

CloudSOC Technical Support articles and alerts including, but not limited to items in the Support Knowledge Base which can be located by logging into your CloudSOC UI and navigating to the Support ticket icon and then selecting **View old tickets** as displayed in the image below:



Note: If you have logged into the CloudSOC UI using a Single Sign-on mechanism, that you will not be auto-redirected to the support knowledge base. You will need to log in with your CloudSOC credentials for this to work.

Symantec CloudSOC Documentation Library
This includes all administration guides and release notes and can be accessed by clicking on the book icon next to the ticket one as seen in the image below:



Symantec recommends you review the following documents in particular:

Release Notes	Up to Version 3.126
User Guides: Gateway	Configuring Client Devices for Traffic Steering Configuring Custom Apps Encrypting your files with the Elastica Gateway Reach Agent Setup for Windows and Mac
User Guides: Audit	Using the Audit App Using Audit for Mobile Apps Discovery

	Managing Data Sources for the CloudSOC Audit App Integrating Blue Coat WSS with Elastica Audit Whitelisting SFTP and SCP IP Addresses Installing and Configuring SpanVA
User Guides: Detect	Using the Detect App
User Guides: Investigate	Using the Investigate App
User Guides: Protect	Using the Protect App Using ContentIQ Using CloudSOC CASB with Symantec DLP Using CloudSOC Threat Protection
User Guides: Securlets	Using the Securlet Dashboards Securlet Editions and Privileges
User Guides: Dashboard	Using the CloudSOC Status Page Customizing CloudSOC Dashboards
User Guides: Administration	Using CloudSOC Accessibility Features Managing CloudSOC Metadata Archiving Administering CloudSOC Users and Groups Encrypting Your Files with Symantec Information Centric Encryption CloudSOC Account Expiration Process
User Guides: API	Delivering CloudSOC Logs with the SIEM Agent CloudSOC Management API

Website

- https://www.broadcom.com/products/cyber-security/information-protection/cloud-application-security-cloudsoc
- https://www.broadcom.com/support/education/software/training-courses
- https://www.broadcom.com/support/education/symantec/elibrary

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.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

Exam Objectives	Applicable Course Content
Demonstrate understanding of the benefits and challenges of cloud applications	• **Course:** CloudSOC Administration R2 • **Modules**: ○ Introduction to Symantec CloudSOC ○ Identifying and Addressing Potential Risk in Cloud Applications • **Documentation**: ○ 2018 Shadow Data Report https://docs.broadcom.com/doc/2018-shadow-date-report-en ○ Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach $260 Billion in 2017 https://www.gartner.com/en/newsroom/press-releases/2017-10-12-gartner-forecasts-worldwide-public-cloud-services-revenue-to-reach-260-billionin-2017 ○ Internet Security Threat Report Volume 22 https://docs.broadcom.com/doc/istr-22-2017-en ○ Internet Security Threat Report Volume 23 https://docs.broadcom.com/doc/istr-23-2018-executive-summary-en-aa ○ Magic Quadrant for Cloud Access Security Brokers October 2019 https://www.gartner.com/doc/reprints?id=1-1XOFK4OX&ct=191024&st=sb
Demonstrate understanding of the problems that CloudSOC solves	• **Course:** CloudSOC Administration R2 • **Modules**: ○ Introduction to Symantec CloudSOC ○ Identifying and Addressing Potential Risk in Cloud Applications
Demonstrate understanding of the basic architecture of CloudSOC	• **Course:** CloudSOC Administration R2 • **Module**: Introduction to Symantec CloudSOC

Exam Objectives	Applicable Course Content
Demonstrate understanding of how to configure CloudSOC	• **Course:** CloudSOC Administration R2 • **Module**: Configuring the Symantec CloudSOC Portal • **Documentation**: ○ Administering CloudSOC Users and Groups
Demonstrate understanding of cloud applications and their risks	• **Course:** CloudSOC Administration R2 • **Module**: Identifying and Addressing Potential Risk in Cloud Applications • **CloudSOC Administration Labs:** Identifying and Addressing Potential Risk in Cloud Applications • **Documentation**:
Demonstrate understanding of the 'Cloud Application Discovery' and 'Safe Adoption' Lifecycles	• **Course:** CloudSOC Administration R2 • **Module**: Identifying and Addressing Potential Risk in Cloud Applications • **Documentation**: Ensuring safe cloud app adoption with Symantec CloudSOC (https://docs.broadcom.com/doc/shadow-it-discovery-best-practices-guide-en)
Show knowledge of SpanVA installation and configuration requirements	• **Course:** CloudSOC Administration R2 • **Module**: Identifying and Addressing Potential Risk in Cloud Applications • **Documentation**: ○ Managing Data Sources for the CloudSOC Audit App ○ Installing and Configuring SpanVA
Demonstrate understanding of the risks of shadow data and shadow IT	• **Course:** CloudSOC Administration R2 • **Module**: Identifying How Data is Used and Shared in Cloud Applications • **Documentation**: 2018 Shadow Data Report https://docs.broadcom.com/doc/2018-shadow-date-report-en
Demonstrate understanding of Detect and how to configure it	• **Course:** CloudSOC Administration R2 • **Module**: Identifying and Remediating Risky Behavior in Cloud Applications • **CloudSOC Administration Labs:** Identifying and Remediating Risky Behavior in Cloud Applications • **Documentation**: Using the Detect App

Exam Objectives	Applicable Course Content
Reviewing anomalous or unauthorized user activity	• **Course:** CloudSOC Administration R2 • **Modules**: ○ Identifying and Remediating Risky Behavior in Cloud Applications ○ Identifying how Data is Used and Shared in Cloud Applications • **CloudSOC Administration Labs:** ○ Identifying and Remediating Risky Behavior in Cloud Applications ○ Identifying how Data is Used and Shared in Cloud Applications • **Documentation**: ○ Using the Securlet Dashboards ○ Using the Detect App ○ Using the Investigate App
Demonstrate knowledge of how to create content profiles	• **Course:** CloudSOC Administration R2 • **Module**: Protecting Data in Cloud Applications • **CloudSOC Administration Labs:** Protecting Data in Cloud Applications • **Documentation**: ○ Using the Protect App ○ Using ContentIQ
Demonstrate knowledge of how to create policies to restrict information sharing	• **Course:** CloudSOC Administration R2 • **Module**: Protecting Data in Cloud Applications • **CloudSOC Administration Labs:** Protecting Data in Cloud Applications • **Documentation**: ○ Using the Protect App ○ Using ContentIQ
Demonstrate knowledge of how to monitor cloud application usage	• **Course:** CloudSOC Administration R2 • **Module**: Protecting Data in Cloud Applications • **CloudSOC Administration Labs:** Protecting Data in Cloud Applications • **Documentation**: ○ Using the Protect App ○ Using ContentIQ
Demonstrate understanding of the reporting options available in CloudSOC	• **Course:** CloudSOC Administration R2 • **Module**: Understanding Reporting Options in CloudSOC and Third-Party Solutions • **Documentation**: ○ Delivering CloudSOC logs with the SIEM Agent ○ CloudSOC Management API ○ Managing CloudSOC Metadata Archiving

Exam Objectives	Applicable Course Content
Demonstrate understanding of integration points with other Symantec products (including CloudSOC Administration R2, ICE, SEP Mobile, ProxySG, VIP)	• **Course:** CloudSOC Administration R2 • **Modules**: ○ Protecting data in Cloud Applications ○ Identifying How Data is Used and Shared in Cloud Applications ○ Identifying and Addressing Potential Risks in Cloud Applications • **Documentation**: ○ Encrypting Your Files with Symantec Information Centric Encryption ○ Using CloudSOC CASB with Symantec DLP

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. **According to the 2018 Shadow Data Report by Symantec, of all broadly shared files, which category of sensitive data is most likely to be over exposed?**
   a. PCI
   b. HIPAA
   c. PII
   d. PHI

2. **According to the 2018 Shadow Data Report by Symantec, where does the greatest risk of data over-exposure originate?**
   a. Unintentionally high-risk employees (well-meaning insiders)
   b. Intentionally high-risk employees (malicious insiders)
   c. Intentionally malicious outsiders (hackers)
   d. A relaxed corporate security policy

3. **When cloud application adoption bypasses formal processes, what are some of the potentially negative outcomes? Select two (2)**
   a. Lack of visibility into how legally protected data, as well as company sensitive data is shared
   b. Inability to identify user behaviors leading to susceptibility for hacking or account compromise
   c. The cost of the adoption is managed centrally, thus making it more likely to cost more
   d. The application cannot be accessed using BYOD, thus reducing productivity
   e. The user cannot chose whether to leverage corporate or personal credentials to create the account, thus reducing productivity

4. **Users and groups are required for CloudSOC to know which data and accounts to scan. How can this information be populated in CloudSOC?**
   a. csv import, Securlet configuration, Active Directory Sync using SpanVA, and Gatelet User Collection
   b. Manual Creation, Securlet configuration, and Active Directory Sync using SpanVA, and Gatelet User Collection
   c. Manual Creation, .csv import, Securlet configuration, and Active Directory Sync using SpanVA
   d. Manual Creation, .csv import, Active Directory Sync using SpanVA, and Gatelet User Collection

5. **CloudSOC users may be allocated one or more 'roles'. Select the correct**
   a. System Administrator, Security Contact, End User, Data Protection Office (DPO)
   b. System Administrator, Administrator, Security Contact, End User, Data Protection Office (DPO)
   c. System Administrator, Administrator, End User, Data Protection Office (DPO)
   d. System Administrator, Administrator, Security Contact, Data Protection Office (DPO)

6. **When creating user profiles for administration of CloudSOC, which areas of control can you enable or restrict?**
   a. CloudSOC Application access, Cloud Service Configuration, Information Level, Global Settings, and Domain Control

b. Cloud Service Configuration, Information Level, Global Settings, and Domain Control
c. CloudSOC Application access, Configuration, Information Level, Global Settings, and Domain Control
d. CloudSOC Application access, Cloud Service Configuration, Global Settings, and Domain Control

7. **You have a user in your organization with whom you wish to share a specific report, but to whom you do not wish to grant portal access. Where in the CloudSOC UI can you configure a scheduled report to be sent to them?**
   a. Investigate
   b. Protect
   c. Audit
   d. Dashboards

8. **The Audit tool in the CloudSOC UI is able to present security verdicts of cloud applications over a variety of form factors. Which?**
   a. Traditional websites, Android applications, iOS applications and Windows applications
   b. Android applications, iOS applications and Windows applications
   c. Traditional websites, Android applications, and iOS applications
   d. Traditional websites, Windows applications, iOS applications

9. **The CloudSOC Audit Tool rates BRR. What does this abbreviation mean?**
   a. Business Review Rating
   b. Business Readiness Ranking
   c. Business Readiness Rating
   d. Business Review Ranking

10. **Data about cloud applications which drives the BRR is shared by CloudSOC with the Symantec Global Intelligence Network (GIN). This information can be utilized to create policies which additional Symantec product?**
    a. Symantec Web Security Service (WSS)
    b. Symantec Email Security.cloud
    c. Symantec Endpoint Protection (SEP)
    d. Symantec ProxySG

Answer Key:

1. d
2. a
3. a, b
4. c
5. b
6. a
7. d
8. b
9. c
10. d