

100% Money Back
Guarantee

Vendor:Symantec

Exam Code:250-437

Exam Name:Administration of Symantec CloudSOC -
version 1

Version:Demo

QUESTION 1









How does the Securlet module get data?

- A. Firewall and proxies
- B. CloudSOC gateway
- C. Cloud application APIs
- D. CloudSOC gateway and cloud application APIs

Correct Answer: D

QUESTION 2

Refer to the exhibit. What modules are used in the use case "Protect information from accidental and intentional exposure within cloud applications"?

	USE CASES	 Audit	 Detect	 Protect	 Investigate	 Securlets
 1) Cloud Visibility	1.1) Identify and determine business risk of cloud applications being used within the organization					
 2) Data Security	1.2) Determine optimal cloud application adoption based on business risk and cost of ownership.					
	2.2) Identify and understand how information is used within cloud applications					
 3) Threat Protection	2.3) Protect information from accidental and intentional exposure within cloud applications					
	3.1) Identify and remediate malicious behaviour within cloud applications					

- A. Protect and Investigate
- B. Protect, Investigate, and Securlets
- C. Protect and Audit
- D. Protect and Securlets

Correct Answer: A

QUESTION 3

What module should an administrator use to create policies with one click, and send them to the Protect Module?

- A. Detect
- B. Investigate
- C. Audit
- D. Securlet

Correct Answer: D

QUESTION 4

What type of connection should an administrator use when the network is sensitive to the bandwidth consumed by log traffic transfer to CloudSOC?

- A. SCP
- B. SpanVA
- C. AWS S3 Bucket
- D. APIs

Correct Answer: D

QUESTION 5

What Rule Type in ContentIQ profiles do FERPA, GLBA, HIPAA, PCI AND PII belong to?

- A. Regular expressions
- B. Content types
- C. Risk types
- D. Keywords

Correct Answer: B

Reference: <https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-security-forsaas-en.pdf>

QUESTION 6

What policy should an administrator utilize to prevent users from internally sharing files with a group of high risk users?

- A. Access Monitoring
- B. File transfer
- C. Threatscore based
- D. Data exposure

Correct Answer: C

QUESTION 7

What policy should an administrator utilize to prevent users from downloading files from Box.com when they are outside the corporate IP range?

- A. File transfer
- B. File sharing
- C. Data exposure
- D. Access enforcement

Correct Answer: A

QUESTION 8

Refer to the exhibit. An administrator found several incidents like this in the Investigate module.

What type of detector should an administrator modify to reduce the frequency of this type of incident?

Service	Amazon Web Services
User Name	user15 user15
User	user15@elasticaworkshop.com
Severity	critical
Happened At	Nov 20,2017, 7:42:30 PM
Recorded At	Nov 20,2017, 7:42:30 PM
Message	The user ThreatScore is now 99. The score changed to 24 for the incident 'Large volume of download data. 1.10MB. Exceeds 1000.00kB threshold in 1.0 minute(s)'
Object Type	File
Activity Type	Download
Alert ID	plqqS6HAQMuK5_34gwhrJw
Threat Score	99
Updated Time	Nov 20, 2017, 7:42:30 PM

- A. Threshold based
- B. Threats based
- C. Sequence based
- D. Behavior based

Correct Answer: A

QUESTION 9

What step should an administrator complete immediately before being able to classify a cloud application using the cloud application adoption workflow?

- A. Discover Shadow IT

- B. Ensure compliance
- C. Analyze usage
- D. Identify risky apps

Correct Answer: A

QUESTION 10

Which action should an administrator take if a cloud application fails to meet security and compliance requirements, but the business need outweighs the risks?

- A. Sanction
- B. Monitor
- C. Block
- D. Substitute

Correct Answer: B

QUESTION 11

What action should an administrator take if a cloud application has significant risks, but mitigating controls are available?

- A. Sanction
- B. Monitor
- C. Block
- D. Substitute

Correct Answer: A

Reference: <https://www.symantec.com/content/dam/symantec/docs/solution-briefs/shadow-it-discoverybest-practices-guide-en.pdf>

QUESTION 12

What Business Readiness Rating (BRR) category does the subcategory "User Audit Trail" belong to?

- A. Data
- B. Informational
- C. Administrative

D. Business

Correct Answer: C

Reference: <https://www.symantec.com/content/dam/symantec/docs/solution-briefs/shadow-it-discoverybest-practices-guide-en.pdf>