



# 250-437<sup>Q&As</sup>

Administration of Symantec CloudSOC - version 1

## Pass Symantec 250-437 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/250-437.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### 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. Which modules are used in the use case "Determine optimal cloud application adoption based on business risk and cost of ownership"?

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

Correct Answer: B

### QUESTION 3

What data source types does Audit support?

- A. SSH, FTP, Remote desktop
- B. Web upload, SFTP, S3
- C. PDF, DOC, XLS
- D. APIs



Correct Answer: C

---

#### QUESTION 4

Refer to the exhibit. An administrator found this incident in the Investigate module.

What type of policy should an administrator create to get email notifications if the incident happens again?

Service	Google Drive
User	user1@elasticaworkshop.com
Severity	warning
Happened At	Oct 26, 2017, 4:33:28 PM
Recorded At	Oct 26, 2017, 4:36:08 PM
Message	User trashed RFC_MX.txt
Object Type	File
Activity Type	Trash
Name	RFC_MX.txt
Org Unit	395c5912-191c-43ad-870d-fdb6558295cf
Resource ID	0B2qkdsN7cC1XaGt3ZE92RjFzQTA
Parent ID	0B2qkdsN7cC1XSfBrZ3NubTRseDQ
File Size	15 B

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

Correct Answer: B

---

#### QUESTION 5

What is the objective of the Data Exposure policy?

- A. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.
- B. To block users from logging into cloud applications if their ThreatScore is higher than a certain level.
- C. To restrict the direct sharing of documents from cloud applications based both on their content and the characteristics of the user.
- D. To notify the administrator, file owner or acting user and/or to prevent users from sharing documents, either publicly, externally, or internally.



Correct Answer: D

[250-437 VCE Dumps](#)

[250-437 Study Guide](#)

[250-437 Exam Questions](#)