



250-437^{Q&As}

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.pass4itsure.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

Refer to the exhibit. Which CloudSOC module(s) use firewalls and proxies as data sources?

| Data sources |  Audit |  Detect |  Protect |  Investigate |  Securlets |
|-----------------------|---|--|---|---|---|
| Firewalls and proxies | | | | | |
| CloudSOC gateway | | | | | |
| Cloud application API | | | | | |

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

Correct Answer: C

Reference: https://www.niwis.com/downloads/Symantec/Symantec_CloudSOC.pdf

QUESTION 2

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 3

What should an administrator utilize to steer traffic from client devices to the CloudSOC gateway?

- A. SpanVA
- B. ProxySG
- C. The Reach agent
- D. SCP/SFTP

Correct Answer: B

QUESTION 4

What are the four (4) types of detectors?

- A. Threshold based, download/upload based, threats based, and sequence based
- B. Threshold based, behavior based, and sequence based



- C. Threshold based, behavior based, download/upload based, and access control based
- D. Threshold based, behavior based, malware based, and sequence based

Correct Answer: B

Reference: <https://www.symantec.com/content/dam/symantec/docs/solution-briefs/cloud-access-securitybroker-best-practices-guide-en.pdf> (p.13)

QUESTION 5

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

[Latest 250-437 Dumps](#)

[250-437 Study Guide](#)

[250-437 Exam Questions](#)