

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.leads4pass.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

Which type of a policy can perform a user log out from Single Sign On?

- A. Access Monitoring policy
- B. ThreatScore based policy
- C. Access enforcement policy
- D. None of the above

Correct Answer: D

QUESTION 3

What CloudSOC module should an administrator use to identify and remediate malicious behavior within cloud applications?

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

Correct Answer: C

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

An administrator discovers that an employee has been sending confidential documents to a competitor.

What type of policy should the administrator use to block the transmission of files to that domain?

- A. Access monitoring
- B. Data Exposure
- C. File transfer
- D. Access enforcement

Correct Answer: B

[250-437 VCE Dumps](#)

[250-437 Study Guide](#)

[250-437 Exam Questions](#)