250-437Q&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.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

QUESTION 1

What policy should an administrator utilize to allow users access to Office 365, but prevent the extraction of files when their ThreatScore is higher than 30?

A. File transfer

B. Access enforcement

C. ThreatScore based

D. Data exposure

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.ALERT2395.html

QUESTION 2

What type of log upload should an administrator use during production?

A. FTP

B. Web upload

C. SCP/SFTP

D. APIs

Correct Answer: C

QUESTION 3

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 4

How does the Detect module get data?

A. Firewalls and proxies

B. CloudSOC gateway and cloud application APIs

C. Firewalls and proxies, and CloudSOC gateway

D. Cloud application APIs

Correct Answer: C

QUESTION 5

How should an administrator handle a cloud application that is business critical, but is NOT the most secure option?

A. Sanction

B. Monitor

C. Block

D. Review

Correct Answer: B

Reference: https://www.symantec.com/content/dam/symantec/docs/solution-briefs/shadow-it-discoverybest-practices-guide-en.pdf (p.13)