250-437^{Q&As}

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.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 module should an administrator use to identify anomalous user behavior such as large amounts of data being downloaded, too many files being shared, or logins from suspicious locations?

A. Detect

B. Protect

C. Investigate

D. Audit

Correct Answer: A

Reference: http://www.arrowecs.pt/ficheros/
partners/211_ShadowDataReport_1H_2016_Digital_Screen_compressed.pdf

QUESTION 2

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 3

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 4

What is the objective of the Access Monitoring policy?

A. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.

B. To restrict the direct sharing of documents from cloud applications based both on their content and the characteristics of the user.

C. To prevent users from sharing documents, either publically, externally, or internally.

D. To restrict the uploading and downloading of documents from the user\\'s computer to the cloud application, based both on the content of the documents and the characteristics of the user.

Correct Answer: A

QUESTION 5

What type of policy should an administrator use to prevent a user that is behaving in anomalous ways from sharing public links while you monitor them?

A. Access monitoring

B. File transfer

C. Data exposure

D. Access enforcement

Correct Answer: D

250-437 PDF Dumps   250-437 Study Guide   250-437 Exam Questions