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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

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

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

Refer to the exhibit. What action should an administrator take if this incident was found in the Investigate module?

Source Location	Sunnyvale (Unites States)
Name	vb_macro.xls
Referrer URI	https://drive.google.com/drive/my-drive
Request URI	https://doc-0c-ag-docs.googleusercontent.com/docs/securesc/0rm1j5aml20ffeu8...
Account Type	Internal
File Size	62.5KB
Risks	VBA Macros
Device :	Mac OS X
Anonymous Proxy	false
City	Sunnyvale
Country	United States
Region	CA
Time Zone	America/Los_Angeles
User Agent	Mozilla/5.O.(Macintosh;Intel Mac OS X 10.12; rv 56.0) Gecko/20100101 Firefox/56.0
Transaction ID	8541da4a-9c30-414f-8c8a-75b54bdd19b1
Threat Prevention	VBA MACROS

Matched Expressions
  (Suspicious-keywords)
    (Module1.bas::ActiveWorkbook.SaveAs (May save the current workbook)

A. Create an access enforcement policy and block access to the file

B. Create a file transfer policy and block the download of the file

C. Create a file sharing policy and block the sharing of the file

D. Create an access monitoring policy and monitor the usage of the file

Correct Answer: D

QUESTION 4

What CloudSOC module should an administrator use to identify and understand how information is used within cloud applications?

A. Investigate

B. Securlets

C. Audit

D. Detect

Correct Answer: C

QUESTION 5

What module should an administrator use to compare firewall logs to a database to identify risky cloud applications?

A. Securlets

B. Detect

C. Protect

D. Audit

Correct Answer: D

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-audit-en.pdf

250-437 PDF Dumps   250-437 Practice Test   250-437 Braindumps