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.passapply.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 type of solution should an administrator implement to secure the way users interact with cloud applications?

A. Intrusion Detection System/Intrusion Protection System (IDS/IPS)

B. Cloud Access Security Broker (CASB)

C. Web application firewalls

D. Proxies

Correct Answer: B

QUESTION 2

Refer to the exhibit. An administrator found several incidents like this in the Investigate module.

What type of detector should an administrator modify to reduce the frequency of this type of incident?

Service	Amazon Web Services
User Name	user15 user15
User	user15@elasticaworkshop.com
Severity	critical
Happened At	Nov 20,2017, 7:42:30 PM
Recorded At	Nov 20,2017, 7:42:30 PM
Message	The user ThreatScore is now 99. The score changed to 24 for the incident 'Large volume of download data. 1.10MB. Exceeds 1000.00kB threshold in 1.0 minute(s)'
Object Type	File
Activity Type	Download
Alert ID	plqqS6HAQMuK5_34gwhrJw
Threat Score	99
Updated Time	Nov 20, 2017, 7:42:30 PM

A. Threshold based

B. Threats based

C. Sequence based

D. Behavior based

Correct Answer: A

QUESTION 3

Which CloudSOC module is similar to a Data Loss Prevention (DLP) system?

A. Detect

B. Investigate

C. Audit

D. Protect

Correct Answer: A

QUESTION 4

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 5

Which are three (3) levels of data exposure?

A. Public, external, and internal

B. Public, confidential, and company confidential

C. Public, semi-private, and private

D. Public, confidential, and private

Correct Answer: A