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.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

QUESTION 1

What CloudSOC module should an administrator use to prevent the accidental and intentional exposure of information within cloud applications?

A. Detect

B. Audit

C. Protect

D. Investigate

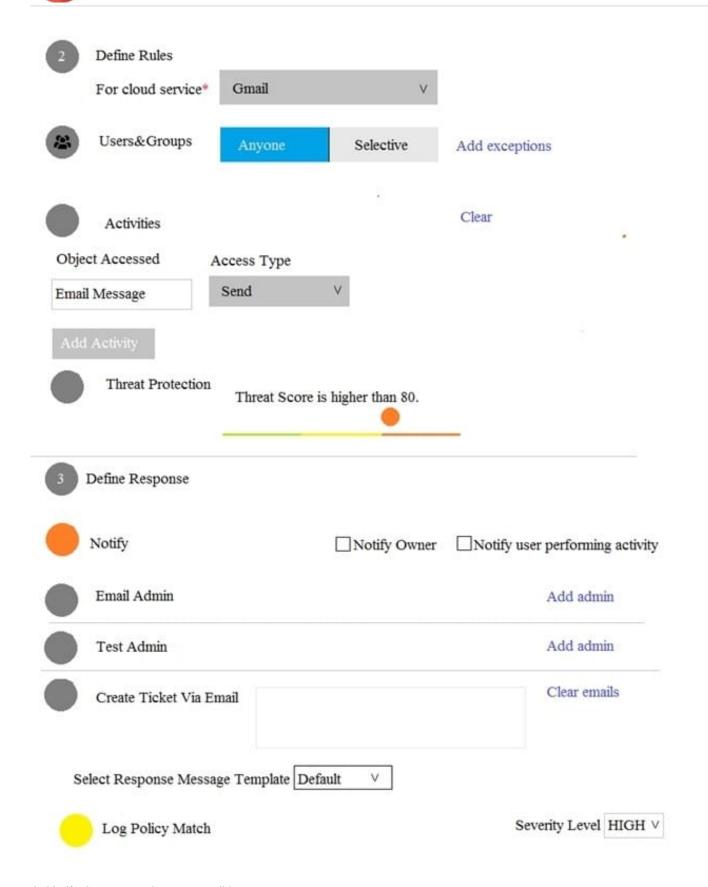Correct Answer: C

QUESTION 2

Refer to the exhibit. What does this Access Monitoring policy do?

2 Define Rules

For cloud service*   Gmail   ∨

👥 Users&Groups   Anyone   Selective   Add exceptions

⬤ Activities   Clear

Object Accessed   Access Type

Email Message   Send   ∨

Add Activity

⬤ Threat Protection   Threat Score is higher than 80.

⬤

3 Define Response

⬤ Notify   ☐ Notify Owner   ☐ Notify user performing activity

⬤ Email Admin   Add admin

⬤ Test Admin   Add admin

⬤ Create Ticket Via Email   Clear emails

Select Response Message Template Default ∨

⬤ Log Policy Match   Severity Level HIGH ∨

A. Notify the owner when an email is sent

B. Send a ticket when a user with a ThreatScore higher than 80 performs an invalid login

C. Notify the admin when a folder is deleted by a user with a ThreatScore higher than 80

D. Create a ticket when a user with a ThreatScore higher than 80 sends an email

Correct Answer: D

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 should an administrator handle a cloud application that fails to meet compliance requirements, but the business need outweighs the risk?

A. Sanction

B. Monitor

C. Block

D. Review

Correct Answer: D

QUESTION 5

Where should an administrator locate unshared content within the Securlet module that contains risky information?

A. Exposed content

B. Activities

C. Other Risks

D. Apps

Correct Answer: B