



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

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 Email Message

Access Type 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 2

Refer to the exhibit. Which module(s) are utilized in the use case "Identify and understand how information is used within cloud applications"?

	USE CASES	 Audit	 Detect	 Protect	 Investigate	 Securlets
 1) Cloud Visibility	1.1) Identify and determine business risk of cloud applications being used within the organization					
 2) Data Security	1.2) Determine optimal cloud application adoption based on business risk and cost of ownership.					
	2.2) Identify and understand how information is used within cloud applications					
 3) Threat Protection	2.3) Protect information from accidental and intentional exposure within cloud applications					
	3.1) Identify and remediate malicious behaviour within cloud applications					

- A. Investigate
- B. Securlets
- C. Protect, Investigate, and Securlets
- D. Detect, Protect, and Investigate

Correct Answer: C

QUESTION 3

Which CloudSOC module is similar to an Intrusion Protection System (IPS)/Intrusion Detection System (IDS)?

- A. Protect
- B. Investigate
- C. Detect
- D. Audit

Correct Answer: A

QUESTION 4

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 5

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

- A. FTP
- B. Web upload
- C. SCP/SFTP
- D. APIs

Correct Answer: C

[250-437 PDF Dumps](#)

[250-437 Exam Questions](#)

[250-437 Braindumps](#)