

# 250-437<sup>Q&As</sup>

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



# https://www.passapply.com/250-437.html

2024 Latest passapply 250-437 PDF and VCE dumps Download

#### **QUESTION 1**

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 2**

What Business Readiness Rating (BRR) category does the subcategory "User Audit Trail" belong to?

- A. Data
- B. Informational
- C. Administrative
- D. Business

Correct Answer: C

Reference: https://www.symantec.com/content/dam/symantec/docs/solution-briefs/shadow-it-discoverybest-practices-guide-en.pdf

# https://www.passapply.com/250-437.html

2024 Latest passapply 250-437 PDF and VCE dumps Download

#### **QUESTION 3**

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					
	1.2) Determine optimal cloud application adoption based on business risk and cost of ownership.					
2) Data Security	$2.2)$ Identify and understand how information is used within cloud applications $% \left( 1\right) =\left( 1\right) $					
	2.3) Protect information from accidental and intentional exposure within cloud applications					
3) Threat Protection	3.1) Identify and remediate malicious behaviour within cloud applications					

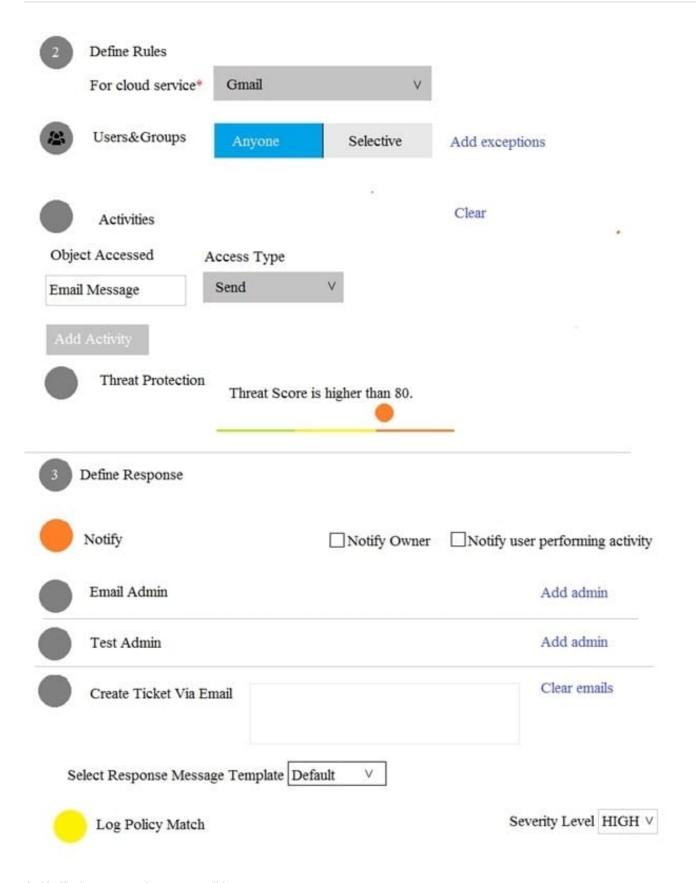
- A. Investigate
- B. Securlets
- C. Protect, Investigate, and Securlets
- D. Detect, Protect, and Investigate

Correct Answer: C

#### **QUESTION 4**

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

### https://www.passapply.com/250-437.html 2024 Latest passapply 250-437 PDF and VCE dumps Download



- 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



## https://www.passapply.com/250-437.html 2024 Latest passapply 250-437 PDF and VCE dumps Download

- 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 5**

What Rule Type in ContentIQ profiles do FERPA, GLBA, HIPAA, PCI AND PII belong to?

- A. Regular expressions
- B. Content types
- C. Risk types
- D. Keywords

Correct Answer: B

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

Latest 250-437 Dumps

250-437 Practice Test

250-437 Study Guide