250-437Q&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.pass2lead.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

Which detector will trigger if CloudSOC detects anomalously frequent sharing?

A. Behavior based

B. Threshold based

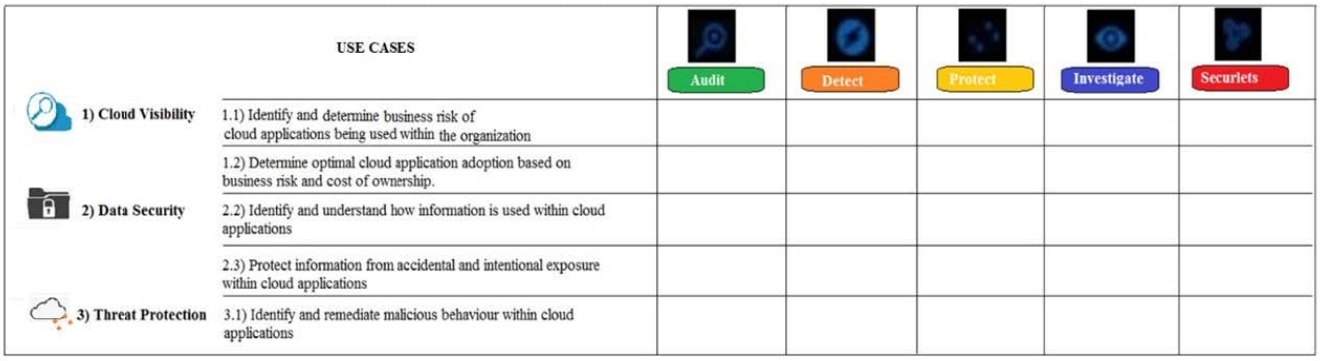
C. Sequence based

D. Threats based

Correct Answer: D

QUESTION 2

Refer to the exhibit. Which modules are used in the use case "Determine optimal cloud application adoption based on business risk and cost of ownership"?



A. Audit and Protect

B. Audit

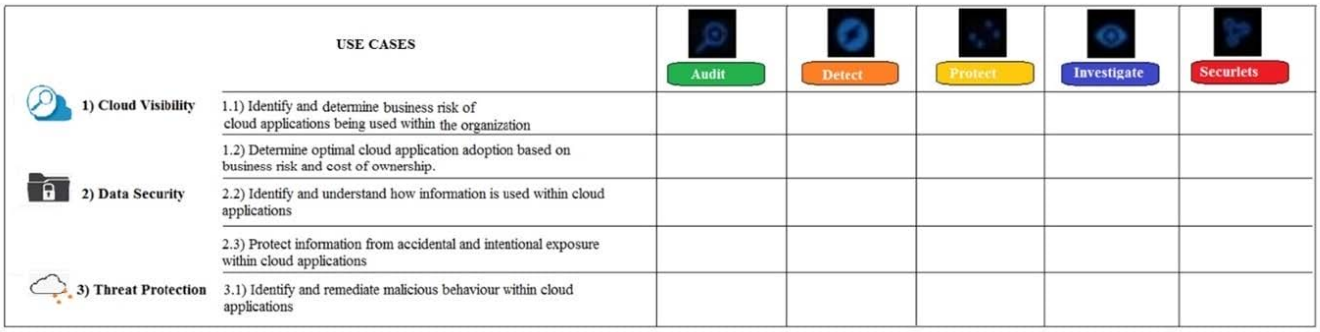
C. Detect, Protect, and Investigate

D. Protect, Investigate, and Securlets

Correct Answer: B

QUESTION 3

Refer to the exhibit. What modules are used by the use case "Identify and determine business risk of cloud applications being used within the organization"?



A. Investigate

B. Audit and Investigate

C. Audit

D. Audit and Securlets

Correct Answer: B

QUESTION 4

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

QUESTION 5

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

250-437 Practice Test 250-437 Study Guide 250-437 Braindumps