Symantec

250-437 Exam

Symantec Administration of Symantec CloudSOC – version 1 Exam

Questions & Answers
Demo

Version: 8.0

Question: 1

How does the audit module get data?

A. Firewall and proxies
B. Cloud application APIs
C. CloudSOC gateway
D. Manual uploads

Answer: B

Question: 2

Which detector will trigger if CloudSOC detector frequent sharing/

A. Behavior based
B. Threshold based
C. Sequence based
D. Threats based

Answer: B

Question: 3

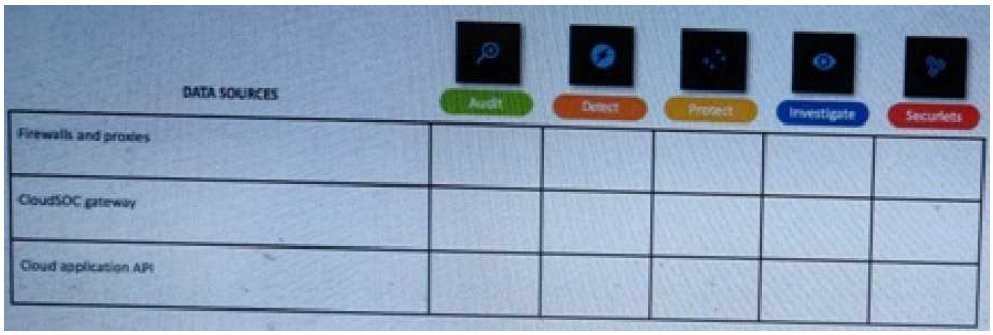
What are three (3) levels of data exposure?

A. Public, external, and internal
B. Public, confidential, and company confidential
C. Public, semi-private, and private
D. Public, confidential, and private

Answer: B

Question: 4

Refer to the exhibit.



Which CloudSOC module(s) use firewalls and proxies as data sources?

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

Answer: B

Question: 5

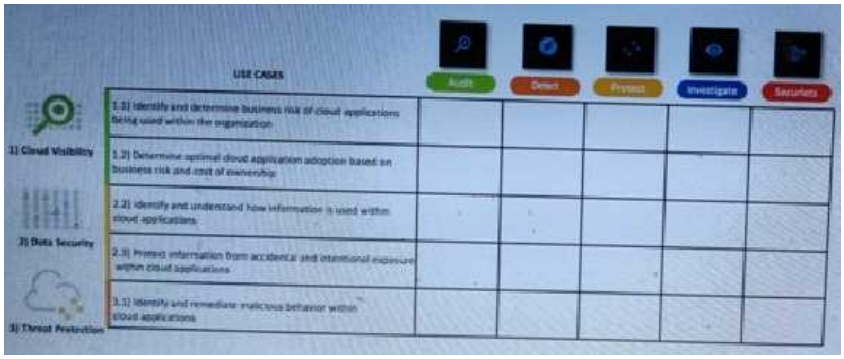
How should an administrator handle a cloud application that fails to meet compliance requirements, but the business need outweighs the risk?

A. Sanction
B. Monitor
C. Block
D. Review

Answer: A

Question: 6

Refer to the exhibit.



What modules are used in the case ''Protect information accidental and intentional exposure within cloud application''?

A. Protect and investigate

B. Protect, Investigate, and Securlets
C. Protect and Audit
D. protect Securlets

Answer: A

Question: 7

What type of policy should an administrator use to a prevent a user that is behaving in anomalous ways from sharing public links while monitor them?

A. Access monitoring
B. File transfer
C. Data exposure
D. Access enforcement

Answer: A