TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate! Testhorse provides update free of charge in one year!

Exam : 250-437

Title : Administration of Symantec

CloudSOC

Version: DEMO

- 1. How does the Audit module get data?
- A. Firewalls and proxies
- B. Cloud application APIs
- C. CloudSOC gateway
- D. Manual uploads

Answer: A

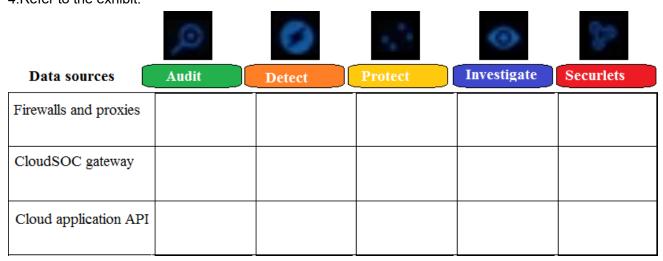
- 2. Which detector will trigger if CloudSOC detects anomalously frequent sharing?
- A. Behavior based
- B. Threshold based
- C. Sequence based
- D. Threats based

Answer: D

- 3. Which 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: A

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: C Explanation:

Reference: https://www.niwis.com/downloads/Symantec/Symantec CloudSOC.pdf

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: D