Vendor: Symantec

Exam Code:250-437

Exam Name: Administration of Symantec CloudSOC - version 1

Version: Demo

QUESTION 1

Where should an administrator locate the level of exposure in files in the Securlet module?

A. Exposure level

B. Exposed files

C. Exposed content

D. Exposure summary

Correct Answer: A

QUESTION 2

What categories should an administrator utilize to classify cloud applications during the cloud applications adoption workflow?

A. Accept, Reject, Block

B. Accept, Monitor, Block

C. Valid, Invalid, In Process

D. Sanction, Monitor, Block

Correct Answer: D

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

---

QUESTION 3

What are the four (4) types of detectors?

A. Threshold based, download/upload based, threats based, and sequence based

B. Threshold based, behavior based, and sequence based

C. Threshold based, behavior based, download/upload based, and access control based

D. Threshold based, behavior based, malware based, and sequence based

Correct Answer: B

Reference: https://www.symantec.com/content/dam/symantec/docs/solution-briefs/cloud-access-securitybroker-best-practices-guide-en.pdf (p.13)

QUESTION 4

What module can an administrator use to connect certain cloud applications to CloudSOC via APIs, and have complete visibility into the content being shared in those cloud applications?

A. Investigate

B. Detect

C. Protect

D. Securlets

Correct Answer: D

QUESTION 5

Who causes 80% of data leaks?

A. Hackers

B. Careless users

C. Malicious insiders

D. System administrators

Correct Answer: C

QUESTION 6

What module should an administrator utilize to identify inherent risk in cloud applications?

A. Investigate

B. Audit

C. Detect

D. Protect

Correct Answer: A

QUESTION 7

What module requires administrative rights to make connections to cloud applications?

A. Securlets

B. Gatelets

C. Audit

D. Investigate

Correct Answer: B

QUESTION 8

Which CloudSOC module should an administrator utilize to identify and understand how cloud applications use information?

A. Audit

B. Detect

C. Securlets

D. Protect

Correct Answer: A

QUESTION 9

Which CloudSOC module(s) use cloud application APIs as data sources?

A. Detect, Protect, Investigate, and Securlets

B. Audit

C. Detect, Protect, and Investigate

D. Investigate and Securlets

Correct Answer: D

QUESTION 10

Which detector will trigger if a user attempts a series of invalid logins within a specific time period?

A. Threats based

B. Sequence based

C. Threshold based

D. Behavior based

Correct Answer: C

QUESTION 11

What policy should an administrator utilize to prevent users from downloading files from Box.com when they are outside the corporate IP range?

A. File transfer

B. File sharing

C. Data exposure

D. Access enforcement

Correct Answer: A

QUESTION 12

What module should an administrator use to compare firewall logs to a database to identify risky cloud applications?

A. Securlets

B. Detect

C. Protect

D. Audit

Correct Answer: D

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