250-437$^{Q\&As}$

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.pass4itsure.com/250-437.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

QUESTION 1

What is the objective of the Data Exposure policy?

A. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.

B. To block users from logging into cloud applications if their ThreatScore is higher than a certain level.

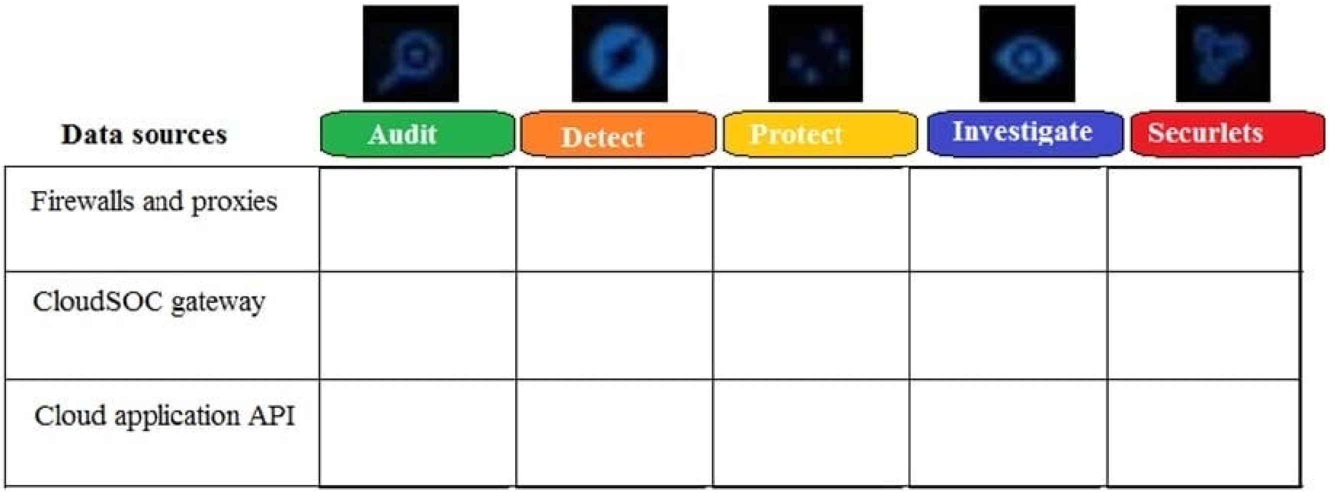
C. To restrict the direct sharing of documents from cloud applications based both on their content and the characteristics of the user.

D. To notify the administrator, file owner or acting user and/or to prevent users from sharing documents, either publicly, externally, or internally.

Correct Answer: D

QUESTION 2

Refer to the exhibit. Which module(s) use the CloudSOC gateway as a data source?



Data sources	Audit	Detect	Protect	Investigate	Securlets
Firewalls and proxies					
CloudSOC gateway					
Cloud application API					

A. Audit

B. Detect and Protect

C. Detect, Protect, and Investigate

D. Detect, Protect, Investigate, and Securlets

Correct Answer: B

QUESTION 3

What compensatory control should an administrator implement if password quality rules of a cloud application has a low rating?

A. Single Sign On (SSO)

B. Block the application

C. Role based access

D. Biometric access

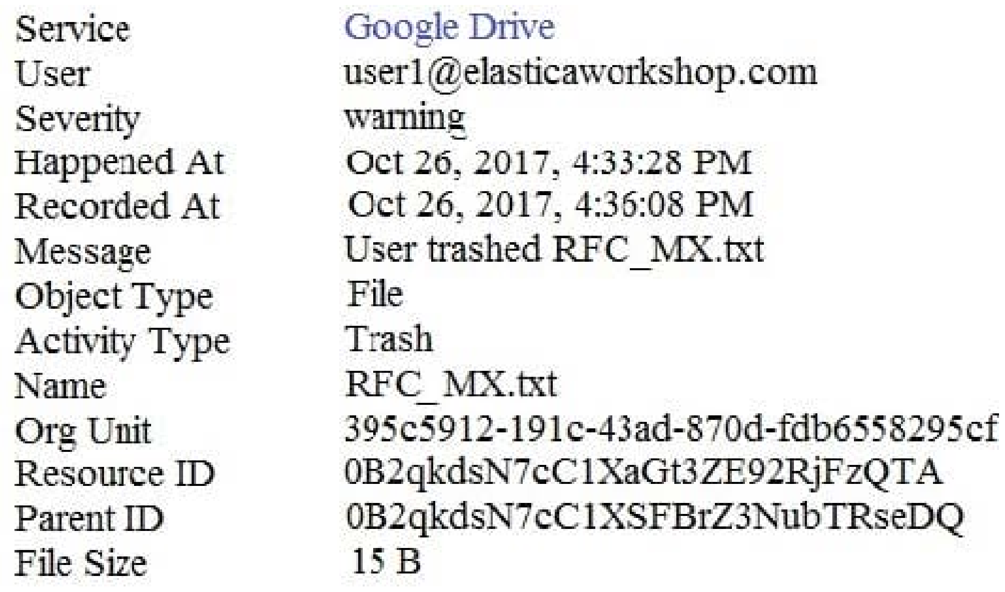
Correct Answer: A

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

QUESTION 4

Refer to the exhibit. An administrator found this incident in the Investigate module.

What type of policy should an administrator create to get email notifications if the incident happens again?



Service	Google Drive
User	user1@elasticaworkshop.com
Severity	warning
Happened At	Oct 26, 2017, 4:33:28 PM
Recorded At	Oct 26, 2017, 4:36:08 PM
Message	User trashed RFC_MX.txt
Object Type	File
Activity Type	Trash
Name	RFC_MX.txt
Org Unit	395c5912-191c-43ad-870d-fdb6558295cf
Resource ID	0B2qkdsN7cC1XaGt3ZE92RjFzQTA
Parent ID	0B2qkdsN7cC1XSFBrZ3NubTRseDQ
File Size	15 B

A. File sharing policy

B. File transfer policy

C. Access monitoring policy

D. Data exposure policy

Correct Answer: B

QUESTION 5

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 6

What action should an administrator take if a cloud application is non-business critical?

A. Sanction

B. Monitor

C. Block

D. Substitute

Correct Answer: C

Reference: https://www.symantec.com/content/dam/symantec/docs/solution-briefs/shadow-it-discoverybest-practices-guide-en.pdf (p.6)

QUESTION 7

What is the objective of File Sharing policies?

A. To restrict the direct sharing of documents from cloud applications based both on their content and the characteristics of the user.

B. To prevent users from sharing documents, either publicly, externally, or internally.

C. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.

D. To restrict the uploading and downloading of documents from the user\\'s computer to the cloud application, based both on the content of the documents, and the characteristics of the user.

Correct Answer: A

QUESTION 8

What type of solution should an administrator implement to secure the way users interact with cloud applications?

A. Intrusion Detection System/Intrusion Protection System (IDS/IPS)

B. Cloud Access Security Broker (CASB)

C. Web application firewalls

D. Proxies

Correct Answer: B

QUESTION 9

What should an administrator do with a cloud application that does NOT meet the compliance requirements, but has mitigating controls available?

A. Sanction

B. Monitor

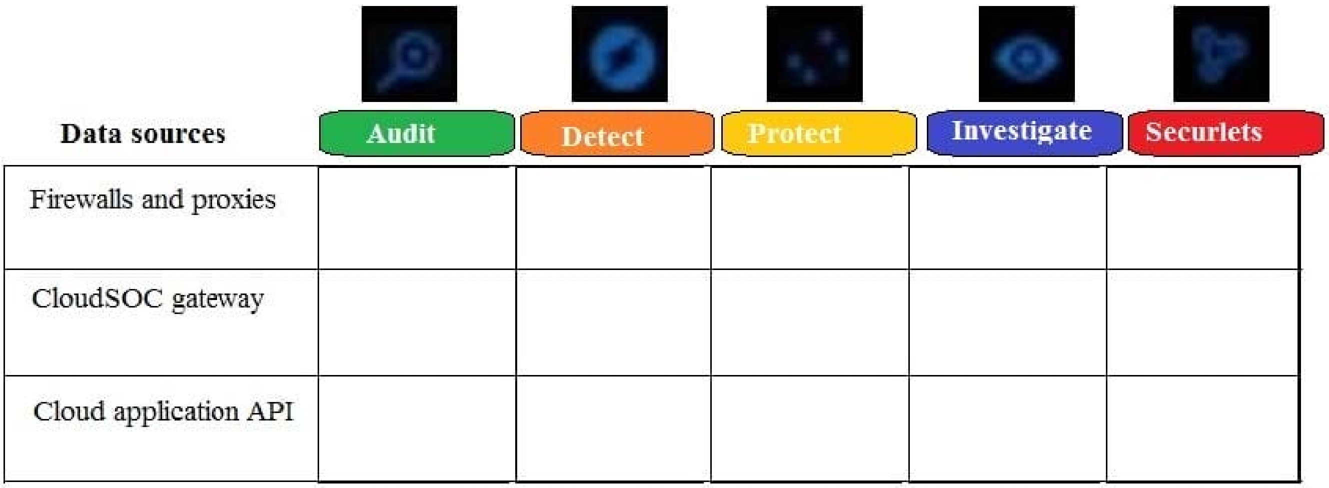
C. Block

D. Review

Correct Answer: A

QUESTION 10

Refer to the exhibit. Which CloudSOC module(s) use firewalls and proxies as data sources?



Data sources	Audit	Detect	Protect	Investigate	Securlets
Firewalls and proxies					
CloudSOC gateway					
Cloud application API					

A. Detect, Protect, and Investigate

B. Detect, Protect, Investigate, and Securlets

C. Audit and Investigate

D. Audit

Correct Answer: C

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

QUESTION 11

What Business Readiness Rating (BRR) category does the subcategory "Password Quality Rules" belong to?

A. Data

B. Compliance

C. Business

D. Access

Correct Answer: D

QUESTION 12

What data source types does Audit support?

A. SSH, FTP, Remote desktop

B. Web upload, SFTP, S3

C. PDF, DOC, XLS

D. APIs

Correct Answer: C

QUESTION 13

What should an administrator use to identify document types specified by the user?

A. Custom dictionaries

B. Training profiles

C. Risk types

D. Content types

Correct Answer: D

QUESTION 14

How does the Securlet module get data?

A. Firewall and proxies

B. CloudSOC gateway

C. Cloud application APIs D. CloudSOC gateway and cloud application APIs

Correct Answer: D

QUESTION 15

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

A. Investigate

B. Audit

C. Detect

D. Protect

Correct Answer: A

250-437 VCE Dumps 250-437 Practice Test 250-437 Exam Questions