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.leads4pass.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 Rule Type in ContentIQ do movies, presentations, raster images, spreadsheets, word processors, and vector graphics belong to?

A. Content format

B. Content types

C. Custom categories

D. File format

Correct Answer: A

QUESTION 2

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 3

What modules are used in the use case "Identify and remediate malicious behavior within cloud applications"?

A. Detect, Protect, and Investigate

B. Detect and Investigate

C. Detect

D. Detect and Securlets

Correct Answer: D

QUESTION 4

What type of policy should an administrator utilize to prevent the spread of malware through cloud applications?

A. Access monitoring

B. File transfer

C. File sharing

D. Access enforcement

Correct Answer: A

QUESTION 5

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 6

Where should an administrator locate unshared content within the Securlet module that contains risky information?

A. Exposed content

B. Activities

C. Other Risks

D. Apps

Correct Answer: B

QUESTION 7

Which CloudSOC module is similar to an Intrusion Protection System (IPS)/Intrusion Detection System (IDS)?

A. Protect

B. Investigate

C. Detect

D. Audit

Correct Answer: A

QUESTION 8

Refer to the exhibit. What action should an administrator take if this incident was found in the Investigate module?

Source Location	Sunnyvale (Unites States)
Name	vb_macro.xls
Referrer URI	https://drive.google.com/drive/my-drive
Request URI	https://doc-0c-ag-docs.googleusercontent.com/docs/securesc/0rm1j5aml20ffeu8...
Account Type	Internal
File Size	62.5KB
Risks	VBA Macros
Device	Mac OS X
Anonymous Proxy	false
City	Sunnyvale
Country	United States
Region	CA
Time Zone	America/Los_Angeles
User Agent	Mozilla/5.O.(Macintosh;Intel Mac OS X 10.12; rv 56.0) Gecko/20100101 Firefox/56.0
Transaction ID	8541da4a-9c30-414f-8c8a-75b54bdd19b1
Threat Prevention	VBA MACROS Matched Expressions (Suspicious-keywords) (Module1.bas::ActiveWorkbook.SaveAs (May save the current workbook)

A. Create an access enforcement policy and block access to the file

B. Create a file transfer policy and block the download of the file

C. Create a file sharing policy and block the sharing of the file

D. Create an access monitoring policy and monitor the usage of the file

Correct Answer: D

QUESTION 9

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 10

Refer to the exhibit. An administrator found several incidents like this in the Investigate module.

What type of detector should an administrator modify to reduce the frequency of this type of incident?

Service	Amazon Web Services
User Name	user15 user15
User	user15@elasticaworkshop.com
Severity	critical
Happened At	Nov 20,2017, 7:42:30 PM
Recorded At	Nov 20,2017, 7:42:30 PM
Message	The user ThreatScore is now 99. The score changed to 24 for the incident 'Large volume of download data. 1.10MB. Exceeds 1000.00kB threshold in 1.0 minute(s)'
Object Type	File
Activity Type	Download
Alert ID	plqqS6HAQMuK5_34gwhrJw
Threat Score	99
Updated Time	Nov 20, 2017, 7:42:30 PM

A. Threshold based

B. Threats based

C. Sequence based

D. Behavior based

Correct Answer: A

QUESTION 11

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 12

What Rule Type in ContentIQ profiles do business, computing, encryption, engineering, health, and legal belong to?

A. Content types

B. Custom dictionaries

C. Keywords

D. Risk types

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-casb-for-iaasen.pdf (p.4)

QUESTION 13

What module should an administrator utilize to view all the activities in cloud applications and conduct analysis?

A. Audit

B. Detect

C. Protect

D. Investigate

Correct Answer: A

QUESTION 14

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 15

Which action should an administrator take if a cloud application fails to meet security and compliance requirements, but the business need outweighs the risks?

A. Sanction

B. Monitor

C. Block

D. Substitute

Correct Answer: B