**Total Question: 74 QAs**

Question: 1
Refer to the exhibit. What does this Access Monitoring policy do?
A. Notify the owner when an email is sent
B. Send a ticket when a user with a ThreatScore higher than 80 perform an invalid login.
C. Notify the admin when a folder is deleted by a user with a ThreatScores higher than 80
D. Create a ticket when a user with a ThreatScore higher than 80 sends an email
Answer: D

Question: 2
What module should and administrator utilize to identify inherent risk in cloud applications?
A. Investigate
B. Audit
C. Detect
D. Protect
Answer: B

Question: 3
How does the audit module get data?
A. Firewall and proxies
B. Cloud application APIs
C. CloudSOC gateway
D. Manual uploads
Answer: B

Question: 4
What Business Readiness Rating (BRR) category does the subcategory "user Audit trail" belong to?
A. Data
B. Informational
C. Administration
D. Business
Answer: C

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.

| | |
|---|---|
| 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 | 0B2akdsN7cC1XaGt3ZE92RjFzQTA |
| Parent ID | 0B2akdsN7cC1XSFBrZ3NubTRseDQ |
| File Size | 15 B |

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?
A. File sharing policy
B. File transfer policy
C. Access monitoring policy
D. Data exposure policy
Answer: C

Question: 7
What modules are used in he use case "identify and remediate malicious behavior within cloud applications"?
A. Detect, Protect, and Investigate
B. Detect and Investigate
C. Detect
D. Detect and Securletss
Answer: A

Question: 8
What CloudSDC module should an administrator use to identify and understand how information is used within cloud applications?
A. Investigate
B. Securlets
C. Audit

D. Detect
Answer: B

Question: 9
What datasource types does Audit support?
A. SSH, FTP, Remote desktop
B. Web upload, SFTP. S3
C. PDF, DOC, XLS
D. APIs
Answer: B

Question: 10
What module requires administrative rights to make connections to cloud application?
A. Securlets
B. Gatelets
C. Audit
D. Investigate
Answer: B

Question: 11
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: 12
What compensatory control should an administrator implement if password quality rules of a cloud application has a low rating?
A. Single Sign (SSO)
B. Block the application
C. Role based access
D. Biometric access
Answer: A

Question: 13
What CloudSOC module should an administrator use to identify and remediate malicious behavior within cloud applications?
A. Audit
B. Securlets
C. Detect
D. Investigate
Answer: C

Question: 14
Refer to the exhibit from the investigate module. What type of policy should an administration utilize to prevent users from accessing files using an unmanaged device?
A. Access enforcement
B. File sharing
C. File transfer
D. Device enforcement
Answer: D

Question: 15
What policy should an administrator utilize to prevent users from internally sharing files with a group of high risk users?
A. Access Monitoring
B. File transfer
C. Threatscore based
D. Data exposure
Answer: A

Question: 16
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. Threahold based
D. Behavior based
Answer: C

Question: 17
What module should an administrator use to create policies with one click, and send them to the Protect Module?
A. Detect
B. Investigate
C. Audit
D. Securlet
Answer: A

Question: 18
An administrator discovers that an employee has been sending confidential document to a competitor. What type of policy should the administrator use top block the transmission of files to that domain?
A. Access monitoring
B. Data Exposure
C. File transfer
D. Access enforcement
Answer: D

Question: 19
What module should an administrator use to view all activities in cloud applications?
A. Protect
B. Audit
C. Detect
D. Investigate
Answer: D

Question: 20
What is the objective of the Access Monitoring policy?
A. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.
B. To restrict the direct sharing of documents from cloud application based both on their content and the characteristics of the user.
C. To prevent users from sharing documents, either publically, externally, or internally.
D. To restrict the uploading and downloading of documents from the user's computers to the cloud application, based both on the content of the documents and the characteristics of the user.
Answer: D

Question: 21
What is the objective of the Access Enforcement policy?
A. To notify an administrator when activities such as objects being modified, are performed in a cloud application.
B. To restrict the direct sharing of document from cloud applications based both on their content and the characteristics of the user.
C. To restrict the uploading and downloading of documents from the user's to the cloud, based both on the content of the documents, and the characteristics of the user.
D. To restrict user access to cloud application not based content, but based on the user's characteristics, such as device and locations.
Answer: A

Question: 22
Which Cloud module should an administrator use to identify and determine business risk of cloud applications within an organization?
A. Investigate
B. Protect
C. Audit
D. Detect
Answer: A

Question: 23
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?