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

Administration of Symantec CloudSOC - version 1

QUESTION 1

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 2

What should an administrator utilize to steer traffic from client devices to the CloudSOC gateway?

A. SpanVA

B. ProxySG

C. The Reach agent

D. SCP/SFTP

Correct Answer: B

QUESTION 3

What is one of the security challenges generated by the proliferation of cloud applications?

A. Variety of endpoints

B. Cross-site scripting

C. Malware

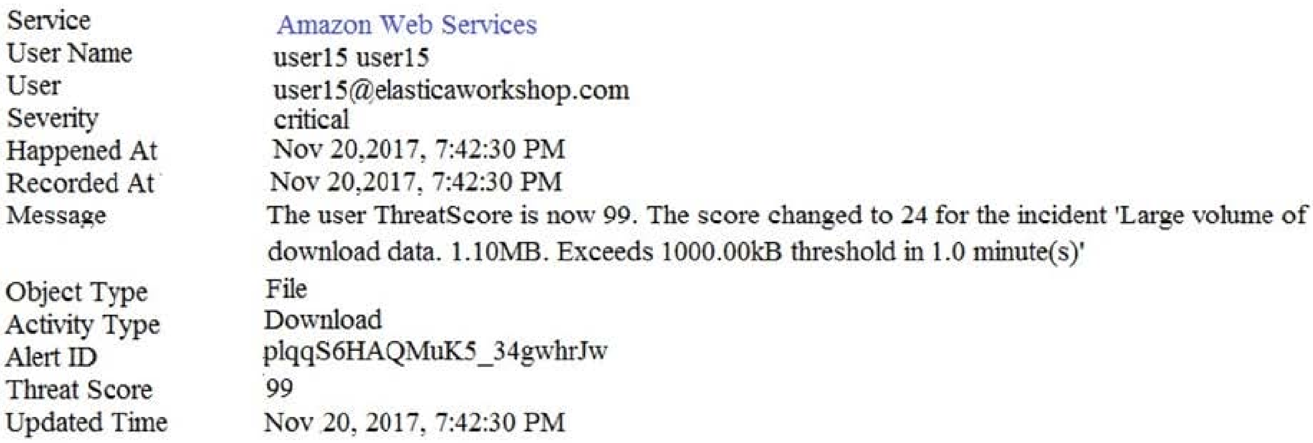
D. Vulnerabilities

Correct Answer: C

QUESTION 4

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 5

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 documents 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 computer to the cloud application, based both on the content of the documents, and the characteristics of the user.

D. To restrict user access to cloud applications not based on content, but based on the user\\'s characteristics, such as devices and locations.

Correct Answer: D