Question: 1

What is the result of creating an exception from an exploit security event?

A. White lists the process from Wild Fire analysis
B. exempts the user from generating events for 24 hours
C. exempts administrators from generating alerts for 24 hours
D. disables the triggered EPM for the host and process involve

Answer: D

Question: 2

What is the retention requirement for Cortex Data Lake sizing?

A. number of endpoints
B. number of VM-Series NGFW
C. number of days
D. logs per second

Answer: C

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/getstarted-
with-cortex-data-lake/set-log-storage-quota

Question: 3

The certificate used for decryption was installed as a trusted toot CA certificate to ensure communication between the Cortex XDR Agent and Cortex XDR Management Console. What action needs to be taken if the administrator determines the Cortex XDR Agents are not communicating with the Cortex XDR Management Console?

A. add paloaltonetworks.com to the SSL Decryption Exclusion list
B. enable SSL decryption
C. disable SSL decryption
D. reinstall the root CA certificate

Answer: D

Question: 4

Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

A. Security Event
B. HIP
C. Correlation
D. Analytics

Answer: AB

Question: 5

Which two items are stitched to the Cortex XDR causality chain'' (Choose two)

A. firewall alert
B. SIEM alert
C. full URL
D. registry set value

Answer: AC