250-441$^{Q\&As}$

Administration of Symantec Advanced Threat Protection 3.0

QUESTION 1

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 2

An Incident Responder is going to run an indicators of compromise (IOC) search on the endpoints and wants to use operators in the expression.

Which tokens accept one or more of the available operators when building an expression?

A. All tokens

B. Domainname, Filename, and Filehash

C. Filename, Filehash, and Registry

D. Domainname and Filename only

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.HOWTO125969.html#v115770112

QUESTION 3

While filling out the After Actions Report, an Incident Response Team noted that improved log monitoring could help detect future breaches.

What are two examples of how an organization can improve log monitoring to help detect future breaches? (Choose two.)

A. Periodically log into the ATP manager and review only the Dashboard.

B. Implement IT Analytics to create more flexible reporting.

C. Dedicate an administrator to monitor new events as they flow into the ATP manager.

D. Set email notifications in the ATP manager to message the Security team when a new incident is occurring.

E. Implement Syslog to aggregate information from other systems, including ATP, and review log data in a single console.

Correct Answer: DE

QUESTION 4

In which scenario should an Incident Responder manually submit a file to the Cynic portal?

A. There is a file on a USB that an Incident Responder wants to analyze in a sandbox.

B. An Incident Responder is unable to remember the password to the .zip archive.

C. The file has generated multiple incidents in the ATP manager and an Incident Responder wants to blacklist the file.

D. The file is a legitimate application and an Incident Responder wants to report it to Symantec as a false positive.

Correct Answer: D

Reference: https://support.symantec.com/content/unifiedweb/en_US/article.HOWTO124806.html

QUESTION 5

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B