Free Questions for 500-275 by ebraindumps

Shared by Taylor on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Advanced custom signatures are written using which type of syntax?

Options:

A- Snort signatures

B- Firewall signatures

C- ClamAV signatures

D- bash shell

Answer:

C

Question 2

Question Type: MultipleChoice

Which set of actions would you take to create a simple custom detection?

Options:

A- Add a SHA-256 value; upload a file to calculate a SHA-256 value; upload a text file that contains SHA-256 values.

B- Upload a packet capture; use a Snort rule; use a ClamAV rule.

C- Manually input the PE header data, the MD-5 hash, and a list of MD-5 hashes.

D- Input the file and file name.

Answer:

A

Question 3

Question Type: **MultipleChoice**

How does application blocking enhance security?

Options:

A- It identifies and logs usage.

B- It tracks application abuse.

C- It deletes identified applications.

D- It blocks vulnerable applications from running, until they are patched.

Answer:

D

Question 4

Question Type: **MultipleChoice**

Custom white lists are used for which purpose?

Options:

A- to specify which files to alert on

B- to specify which files to delete

C- to specify which files to ignore

D- to specify which files to sandbox

Answer:

C

Question 5

Question Type: MultipleChoice

When discussing the FireAMP product, which term does the acronym DFC represent?

Options:

A- It means Detected Forensic Cause.

B- It means Duplicate File Contents.

C- It means Device Flow Correlation.

D- It is not an acronym that is associated with the FireAMP product.

Answer:

C

Question 6

Question Type: MultipleChoice

File information is sent to the Sourcefire Collective Security Intelligence Cloud using which format?

Options:

A- MD5

B- SHA-1

C- filenames

D- SHA-256

Answer:

D