ACTUAL TEST DUMPS

Free Questions for 250-561 by actualtestdumps

Shared by Stephenson on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which antimalware intensity level is defined by the following: "Blocks files that are most certainly bad or potentially bad files. Results in a comparable number of false positives and false negatives."

Options:

A- Level 5

B- Level 2

C- Level 1

D- Level 6

Answer:

D

Question 2

Question Type: MultipleChoice

Which term or expression is utilized when adversaries leverage existing tools in the environment?

Options:

A- opportunistic attack

B- script kiddies

C- living off the land

D- file-less attack

Answer:

B

Question 3

Question Type: **MultipleChoice**

What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)

Options:

A- Increased content update frequency

B- Increased visibility

C- Reduced 3rd party licensing cost

D- Reduced database usage

E- Reduced network usage

Answer:

C, D

Question 4

Question Type: MultipleChoice

Files are blocked by hash in the blacklist policy.

Which algorithm is supported, in addition to MD5?

Options:

A- SHA256

B- SHA256 'salted'

C- MD5 'Salted'

D- SHA2

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which report template type should an administrator utilize to create a daily summary of network threats detected?

Options:

A- Network Risk Report

B- Blocked Threats Report

C- Intrusion Prevention Report

D- Access Violation Report

Answer:

D

Question 6

Question Type: **MultipleChoice**

An administrator selects the Discovered Items list in the ICDm to investigate a recent surge in suspicious file activity. What should an administrator do to display only high risk files?

Options:

A- Apply a list control

B- Apply a search rule

C- Apply a list filter

D- Apply a search modifier

Answer:

B

Question 7

Question Type: MultipleChoice

Which statement best defines Machine Learning?

Options:

A- A program that needs user input to perform a task.

B- A program that teams from observing other programs.

C- A program that learns from experience to optimize the output of a task.

D- A program that require data to perform a task.

Answer:

B

Question 8

Question Type: MultipleChoice

Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?

Options:

A- The Firewall Policy

B- The System Schedule Policy

C- The System Policy

D- The LiveUpdate Policy

Answer:

D

Question 9

Question Type: MultipleChoice

Which IPS Signature type is Primarily used to identify specific unwanted traffic?

Options:

A- Attack

B- Probe

C- Audit

D- Malcode

Answer:

A

Question 10

Question Type: **MultipleChoice**

A user downloads and opens a PDF file with Adobe Acrobat. Unknown to the user, a hidden script in the file begins downloading a RAT.

Which Anti-malware engine recognizes that this behavior is inconsistent with normal Acrobat functionality, blocks the

behavior and kills Acrobat?

Options:

A- SONAR

B- Sapient

C- IPS

D- Emulator

Answer:

B

Question 11

Question Type: **MultipleChoice**

Which dashboard should an administrator access to view the current health of the environment?

Options:

A- The Antimalware Dashboard

B- The SES Dashboard

C- The Device Integrity Dashboard

D- The Security Control Dashboard

Answer:

D