GCED[Q&As]

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.

B. The pass action passes the packet onto further rules for immediate analysis.

C. The pass action serves as a placeholder in the snort configuration file for future rule updates.

D. Using the pass action allows a packet to be passed to an external process.

E. The pass action increases the number of false positives, better testing the rules.

Correct Answer: A

Explanation: The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data. False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible. The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

QUESTION 2

Which control would BEST help detect a potential insider threat?

A. Mandatory approval process for executive and administrative access requests.

B. Providing the same access to all employees and monitoring sensitive file access.

C. Multiple scheduled log reviews of all employee access levels throughout the year

D. Requiring more than one employee to be trained on each task or job duty.

Correct Answer: A

QUESTION 3

From a security perspective, how should the Root Bridge be determined in a Spanning Tree Protocol (STP) environment?

A. Manually selected and defined by the network architect or engineer.

B. Defined by selecting the highest Bridge ID to be the root bridge.

C. Automatically selected by the Spanning Tree Protocol (STP).

D. All switch interfaces become root bridges in an STP environment.

Correct Answer: B

QUESTION 4

Which of the following is considered a preventative control in operational security?

A. Smoke Sensors

B. Fire Suppressant

C. Voltage Regulators

D. Vibration Alarms

Correct Answer: B

Explanation: A fire suppressant device is a preventive control. Smoke sensors, vibration alarms, and voltage regulators are part of detection controls.

QUESTION 5

Which of the following would be used in order to restrict software form performing unauthorized operations, such as invalid access to memory or invalid calls to system access?

A. Perimeter Control

B. User Control

C. Application Control

D. Protocol Control

E. Network Control

Correct Answer: C