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.pass2lead.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

How does data classification help protect against data loss?

A. DLP systems require classification in order to protect data

B. Data at rest is easier to protect than data in transit

C. Digital watermarks can be applied to sensitive data

D. Resources and controls can be appropriately allocated

Correct Answer: A

QUESTION 2

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

A. Stateful packet filtering

B. Signature matching

C. Protocol anomaly detection

D. CRC checking

E. Forward error correction

Correct Answer: C

Explanation: In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

QUESTION 3

Which of the following is the best way to establish and verify the integrity of a file before copying it during an investigation?

A. Write down the file size of the file before and after copying and ensure they match

B. Ensure that the MAC times are identical before and after copying the file

C. Establish the chain of custody with the system description to prove it is the same image

D. Create hash of the file before and after copying the image verifying they are identical

Correct Answer: D

QUESTION 4

Which tasks would a First Responder perform during the Identification phase of Incident Response?

A. Verify the root cause of the incident and apply any missing security patches.

B. Install or reenable host-based firewalls and anti-virus software on suspected systems.

C. Search for sources of data and information that may be valuable in confirming and containing an incident.

D. Disconnect network communications and search for malicious executables or processes.

Correct Answer: C

QUESTION 5

What feature of Wireshark allows the analysis of one HTTP conversation?

A. Follow UDP Stream

B. Follow TCP Stream

C. Conversation list > IPV4

D. Setting a display filter to `tcp\\'

Correct Answer: B

Explanation: Follow TCP Stream is a feature of Wireshark that allows the analysis of a single TCP conversation between two hosts over multiple packets. Filtering packets using tcp in the filter box will return all TCP packets, not grouping by a single TCP conversation. HTTP is TCP not UDP, so you cannot follow a HTTP stream over UDP.