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

Michael, a software engineer, added a module to a banking customer\\'s code. The new module deposits small amounts of money into his personal bank account. Michael has access to edit the code, but only code reviewers have the ability to commit modules to production. The code reviewers have a backlog of work, and are often willing to trust the software developers\\' testing and confidence in the code.

Which technique is Michael most likely to engage to implement the malicious code?

A. Denial of Service

B. Race Condition

C. Phishing

D. Social Engineering

Correct Answer: C

QUESTION 2

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Correct Answer: A

Explanation: By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION 3

Monitoring the transmission of data across the network using a man-in-the-middle attack presents a threat against which type of data?

A. At-rest

B. In-transit

C. Public

D. Encrypted

Correct Answer: B

QUESTION 4

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

A. Monitoring failed authentications on a central logging device

B. Enforcing TLS encryption for outbound email with attachments

C. Blocking email attachments that match the hashes of the company\\'s classification templates

D. Running custom keyword scans on outbound SMTP traffic from the mail server

Correct Answer: D

QUESTION 5

An incident response team is handling a worm infection among their user workstations. They created an

IPS signature to detect and block worm activity on the border IPS, then removed the worm\\'s artifacts or

workstations triggering the rule.

Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm\\'s propagation method

Correct Answer: B

Explanation: Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didn\\'t detect all the infected workstations.