

GIAC GCTI

Cyber Threat Intelligence

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/gcti>

Latest Version: 6.0

Question: 1

During the _____ phase of the Cyber Kill Chain, the adversary exploits a vulnerability to execute code on the victim's system.

Response:

- A. Reconnaissance
- B. Exploitation
- C. Delivery
- D. Installation

Answer: B

Question: 2

Which of the following best describes the concept of "data normalization" in the context of storing threat intelligence data?

Response:

- A. Encrypting data to protect it from unauthorized access
- B. Reducing the amount of data to save storage space
- C. Transforming data into a common format to facilitate analysis and comparison
- D. Compressing data to speed up transmission

Answer: C

Question: 3

Which data storage strategy is most effective for handling large volumes of threat intelligence data from multiple sources?

Response:

- A. Relational databases with strict schema
- B. Encrypted USB drives for portability
- C. Local storage on individual analyst workstations
- D. Distributed storage systems with scalable architecture

Answer: D

Question: 4

In static malware analysis, which of the following techniques are commonly used?

(Select 3)

Response:

- A. Code disassembly
- B. Behavior monitoring
- C. String extraction
- D. Network traffic analysis
- E. File hashing

Answer: A,C,E

Question: 5

When analyzing intelligence, which cognitive bias involves favoring information that confirms preexisting beliefs or theories?

Response:

- A. Availability bias
- B. Confirmation bias
- C. Anchoring bias
- D. Hindsight bias

Answer: B

Question: 6

Which of the following are examples of dynamic analysis tools?

(Select 2)

Response:

- A. OllyDbg
- B. PEiD
- C. Cuckoo Sandbox
- D. IDA Pro

Answer: A,C

Question: 7

How can intelligence from well-known cyber attacks be used to improve current cybersecurity practices?

(Select 3)

Response:

- A. Developing new encryption standards
- B. Understanding attacker tactics
- C. Enhancing incident response plans
- D. Designing user-friendly interfaces
- E. Training staff on social engineering

Answer: B,C,D

Question: 8

The Courses of Action Matrix helps analysts determine the best way to _____ a threat.

Response:

- A. Monitor
- B. Ignore
- C. Respond to
- D. Create

Answer: C

Question: 9

Which of the following is an example of a logical fallacy that could hinder accurate analysis?

Response:

- A. Hasty generalization
- B. Data normalization
- C. Algorithm bias
- D. Redundancy elimination

Answer: A

Question: 10

What are key techniques used in analyzing gathered intelligence?

(Select 3)

Response:

- A. Vulnerability scanning
- B. Intrusion detection
- C. Pattern recognition
- D. Correlation analysis
- E. Trend analysis

Answer: C,D,E

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>