



CERTSWARRIOR

GIAC GSOM

GIAC Security Operations Manager

Questions&AnswersPDF

ForMoreInformation:

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

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.0

Question: 1

Defensible security architecture typically includes which of the following features?

Response:

- A. Single layer of security at the network perimeter
- B. Strong emphasis on endpoint security
- C. Isolation of IT systems for easier management
- D. Neglecting the importance of data encryption

Answer: B

Question: 2

What role does automation play in managing alert processing in a SOC?

Response:

- A. To replace human judgment entirely in alert evaluation
- B. To facilitate faster initial sorting and filtering of alerts
- C. To ensure that every alert is escalated to the highest priority
- D. To eliminate the need for real-time monitoring

Answer: B

Question: 3

Why is it critical to have well-defined roles and responsibilities in incident response?

Response:

- A. To ensure that no one in the organization takes any action, maintaining a clear chain of non-responsibility
- B. To prevent any single point of failure in the response process
- C. To clearly delineate who is to be held accountable for the incident
- D. To assign specific tasks to team members based on their skills and expertise, ensuring efficient and effective response

Answer: D

Question: 4

Analytic testing within SOC operations can help identify:

Response:

- A. The best cybersecurity insurance policies
- B. Future trends in employee behavior
- C. Weaknesses in the incident response plan
- D. The most efficient software update schedules

Answer: C

Question: 5

In SOC design, why is it important to understand potential attack paths?

Response:

- A. To ensure the SOC focuses only on high-profile attack vectors
- B. To develop targeted defense strategies and prioritize monitoring efforts
- C. To eliminate the need for regular threat intelligence
- D. To focus solely on perimeter defense

Answer: B

Question: 6

Effective preparation for incident response should:

(Choose two)

Response:

- A. Involve regular training and awareness for all employees
- B. Include establishing communication protocols and contact lists
- C. Rely solely on automated systems for incident detection and response
- D. Neglect the need for an incident classification scheme

Answer: A,B

Question: 7

Cyber Defense Theory often includes the concept of 'Least Privilege.' What does this mean in practice?

Response:

- A. Giving users the minimum levels of access – or permissions – needed to perform their job functions
- B. Installing the least number of software applications on a system
- C. Using the least expensive cybersecurity tools available
- D. Minimizing the number of staff in the cybersecurity department

Answer: A

Question: 8

Adversarial emulation in SOC optimization helps in:

Response:

- A. Justifying the cybersecurity budget to stakeholders
- B. Testing how well SOC can detect and respond to sophisticated attacks
- C. Reducing the necessity for compliance with industry standards
- D. Eliminating the need for human intervention in cybersecurity

Answer: B

Question: 9

What role do analytics play in SOC operations?

Response:

- A. They are solely used for annual reporting purposes.
- B. They help identify patterns and anomalies in data to improve threat detection.
- C. They reduce the need for human analysts.
- D. They are only relevant for external reporting.

Answer: B

Question: 10

How can the SOC use metrics to improve its strategic planning?

Response:

- A. By only tracking the number of alerts generated
- B. By using metrics to identify trends, gaps, and areas for improvement
- C. By selecting arbitrary metrics that are easy to achieve
- D. By focusing metrics solely on network traffic volumes

Answer: B



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ