Ultimate IT Test Preparation Material

GIAC

GSOM
GIAC Security Operations Manager

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Visit us at

Latest Version: 6.0

Question: 1

Effective alert creation should:
(Select all that apply)
Response:

A. Generate a high volume of alerts to increase the chances of detecting incidents
B. Utilize contextual information to enhance alert relevancy
C. Incorporate thresholds to prevent alert fatigue
D. Be configurable and adaptable over time

Answer: B,C,D

Question: 2

To effectively detect advanced persistent threats (APTs), a SOC should:
(Choose two)
Response:

A. Rely exclusively on signature-based detection
B. Utilize behavioral analysis to identify subtle indicators of compromise
C. Engage in continuous information sharing with similar organizations
D. Assume APTs cannot bypass traditional security measures

Answer: B,C

Question: 3

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: 4

In designing a defensible security architecture, which elements are critical?
(Choose two)
Response:

A. Assuming that all network traffic is benign until proven otherwise
B. Implementing security at different layers (e.g., perimeter, network, host)
C. Regular testing and updates to security controls
D. Relying solely on antivirus software for endpoint protection

Answer: B,C

Question: 5

Which of the following best describes the role of automation in optimizing SOC operations post-incident?
Response:

A. Automates routine tasks to reduce human error
B. Replaces the need for human analysis entirely
C. Increases the incidence of false positives
D. Decreases the speed of incident response

Answer: A

Question: 6

What role does 'Threat Hunting' play in cyber defense?
Response:

A. It passively waits for alerts from other security tools
B. It involves actively looking for indicators of compromise within an environment
C. It is solely focused on external threat intelligence gathering
D. It disregards any anomalous activity that does not match known patterns

Answer: B

Question: 7

Why is it important to integrate endpoint detection and response (EDR) tools into SOC operations?
Response:

A. To monitor and manage desktop environments only
B. To replace the need for a SIEM system
C. To provide detailed visibility into endpoint activities and potential threats
D. To focus solely on external threats and ignore internal anomalies

Answer: C

Question: 8

How can industry frameworks assist in the planning and prioritization of data collection for SOC monitoring?
Response:

A. By providing specific data sources to collect from, regardless of organizational context
B. By offering best practices and standards for structuring data collection
C. By eliminating the need for organizational input
D. By mandating uniform data collection processes across industries

Answer: B

Question: 9

When assessing data sources for SOC monitoring, what is an important consideration related to organizational specific use cases?
Response:

A. Implementing the same use cases across different organizations
B. Customizing data collection methods to fit these use cases
C. Choosing use cases that are easiest to implement, regardless of relevance
D. Avoiding the use of use cases to simplify data collection

Answer: B

Question: 10

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

For More Information – **Visit link below:**

https://www.testsexpert.com/

16$ Discount Coupon: 9M2GK4NW

Features:

- Money Back Guarantee……..……...…. 

- 100% Course Coverage…… 

- 90 Days Free Updates…… 

- Instant Email Delivery after Order……