GIAC

GSOC

GIAC Security Operations Certified

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.1

Question: 1

What advantage does integrating a Threat Intelligence Platform with a SIEM offer to a SOC?
Response:

A. It allows the SOC to broadcast threat alerts on television.
B. It enables correlation of external threat data with internal event data for enhanced analysis.
C. It transforms the SIEM into an autonomous AI entity.
D. It provides a direct marketing channel to potential clients.

Answer: B

Question: 2

Which of the following best describes the concept of 'orchestration' in cybersecurity?
Response:

A. The manual process of responding to incidents one by one
B. The coordination of various security tools and processes to work together effectively
C. The elimination of all automated tools to enhance human skillsets
D. Focusing solely on external threats without considering internal processes

Answer: B

Question: 3

Why is it important for Blue Teams to continuously update and refine their automation workflows?
Response:

A. To keep pace with the rapidly changing threat landscape
B. To ensure that workflows become increasingly complex and harder to understand
C. To reduce their reliance on technology in favor of manual processes
D. To increase the time spent on each incident for thorough investigation

Answer: A

Question: 4

During the sharing phase of analytics, what is an effective practice for fostering understanding and engagement among stakeholders?
(Choose Three)
Response:

A. Utilizing interactive visualizations
B. Providing detailed technical documentation to all stakeholders regardless of their background
C. Tailoring the presentation to the audience's level of expertise
D. Offering actionable insights based on the data
E. Limiting access to data to prevent information overload

Answer: A,C,D

Question: 5

In the context of endpoint security, why is user training essential?
Response:

A. Users need to understand how to bypass security features when they find them inconvenient.
B. Educated users are less likely to fall victim to phishing attacks that could compromise endpoints.
C. Training allows users to take over the IT department's responsibilities for endpoint security.
D. Users prefer to be part of technical troubleshooting processes.

Answer: B

Question: 6

What is the primary function of a Security Information and Event Management (SIEM) system in a SOC?
Response:

A. To enforce access controls and prevent unauthorized data access
B. To provide a platform for storing and analyzing log data
C. To physically secure the SOC's hardware
D. To manage the payroll for cybersecurity personnel

Answer: B

Question: 7

Which factor is crucial when prioritizing incident response?
Response:

A. The phase of the moon
B. The incident’s potential impact on the organization
C. The personal interest of the responding analyst
D. The geographic location of the attacker

Answer: B

Question: 8

In the context of analytics enrichment, which of the following is considered a best practice?
Response:

A. Ignoring data source reliability
B. Incorporating external data sources for enhanced insights
C. Using only internal data to avoid external biases
D. Enriching data at random intervals

Answer: B

Question: 9

Why is it critical to have an understanding of the layered architecture of enterprise networks when analyzing network traffic?
Response:

A. It aids in understanding where bottlenecks can occur.
B. It is only necessary for designing network infrastructure, not for analysis.
C. Knowledge of different layers helps in pinpointing the source and nature of network issues.
D. It is essential for legal compliance in many jurisdictions.

Answer: C

Question: 10

In Linux, which command can be used to view the real-time updating log file?
Response:

A. cat
B. grep
C. tail -f
D. less

Answer: C