



CERTSWARRIOR

GIAC

GSOC
GIAC Security Operations Certified

Questions & Answers PDF

For More Information:

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

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

Which two sources of information are critical for analyzing Windows system events?

(Choose Two)

Response:

- A. The Application log in Event Viewer
- B. The Security log in Event Viewer
- C. The Recycle Bin's metadata
- D. The Windows Update log

Answer: A,B

Question: 2

For effective network traffic analysis, what should be considered when monitoring encrypted traffic?

(Choose Three)

Response:

- A. The increase in CPU usage due to encryption and decryption processes
- B. The possibility of encrypted malware communication
- C. The certificate authority (CA) issuing the certificates
- D. Establishing baselines for normal encrypted traffic patterns
- E. Ignoring encrypted traffic as it is always secure

Answer: B,C,D

Question: 3

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: 4

When securing endpoints, which two measures are effective in preventing unauthorized access?

(Choose Two)

Response:

- A. Enabling auto-run features for external media
- B. Implementing full disk encryption
- C. Applying strong, unique passwords for each endpoint
- D. Allowing users to install their applications to ensure they have tools they prefer

Answer: B,C

Question: 5

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: 6

How do Threat Intelligence Platforms (TIPs) enhance the effectiveness of a SOC?

Response:

- A. By replacing the need for human analysts
- B. By providing actionable intelligence on emerging threats
- C. By functioning as the primary data storage solution
- D. By automating all incident response actions

Answer: B

Question: 7

Why is it crucial to secure SSH communications, particularly for administrative access?

Response:

- A. Because SSH does not support strong encryption
- B. Because unsecured SSH can provide an attacker with elevated privileges and access to sensitive areas of the network
- C. Because SSH is commonly used over untrusted networks
- D. Because securing SSH is mandated by all data protection regulations

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

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: 10

What is a crucial factor in a SOC's success in improving an organization's security posture?

Response:

-
- A. Isolating the SOC team from the rest of the IT department to avoid biases
 - B. Conducting regular and comprehensive training for SOC staff
 - C. Limiting the SOC's access to essential systems only
 - D. Focusing exclusively on external threat intelligence

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