CERTSWARRIOR

GIAC

GCDA
GIAC Certified Detection Analyst

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 factors should be considered when monitoring logs for assets?
(Choose two)
Response:

A. The criticality of the assets being monitored.
B. The favorite colors of the security analysts.
C. The geographic location of the assets.
D. The compliance requirements related to the assets.

Answer: A,D

Question: 2

How can alert analysis identify staff training opportunities?
Response:

A. By determining which alerts are ignored or mishandled by staff.
B. By tracking the number of alerts generated per day.
C. By calculating the mean time to resolve alerts across the team.
D. By assessing the frequency of alerts during off-hours.

Answer: A

Question: 3

What purposes do detection dashboards serve in log output analysis?
(Select all that apply)
Response:

A. To consolidate and summarize key findings from log data.
B. To provide interactive mechanisms for deeper investigation of alerts.
C. To recommend culinary dishes based on log patterns.
D. To facilitate real-time monitoring and situational awareness.

Answer: A,B,D

Question: 4

What are key considerations in planning storage requirements for log collection?
(Choose two)
Response:

A. The retention period for different types of logs.
B. The resolution of the monitors used to view the logs.
C. The anticipated growth in data volume.
D. The number of users who will access the logs.

Answer: A,C

Question: 5

Why is it beneficial to use virtual machines for post-mortem analysis?
Response:

A. To ensure the analysis environment can be easily replicated or restored.
B. To enhance the graphical interface of the analysis tools.
C. To improve the coffee-making process for analysts.
D. To increase the office space for post-mortem analysts.

Answer: A

Question: 6

Why is it important to analyze user logon patterns in behavior analytics?
Response:

A. To design personalized desktop themes for users.
B. To identify potential unauthorized access or compromised credentials.
C. To select appropriate background music for user logon events.
D. To forecast the cafeteria menu based on user preferences.

Answer: B

Question: 7

In the context of network service log collection, what aspects should be enriched to improve log analysis?
(Choose two)
Response:

A. User and entity behavior analytics (UEBA) for identifying insider threats.
B. Geo-location information to trace the origin of network traffic.
C. Font styles to highlight different levels of log importance.
D. Sound effects to indicate the severity of log events.

Answer: A,B

Question: 8

How does analyzing logs help in identifying attacks specifically in Linux environments?
Response:

A. By detecting unusual access patterns to sensitive files.
B. By tracking the uptime of the system.
C. By monitoring the version control history of deployed applications.
D. By observing the frequency of system reboots.

Answer: A

Question: 9

What is a source collection methodology in the context of software monitoring?
Response:

A. A technique to gather information on the provenance and purpose of installed software.
B. A strategy to collect the best desktop wallpapers from various sources.
C. A method to compile the greatest hits of software-related music.
D. A system to categorize software by the color of its icon.

Answer: A

Question: 10

How can monitoring software help in identifying unauthorized software?
(Choose two)
Response:

A. By maintaining an inventory of authorized applications and alerting on deviations.
B. By playing alert tones in different musical keys based on the software category.
C. By scanning system directories and comparing found applications against a whitelist.
D. By changing the desktop theme when unauthorized software is detected.

Answer: A,C

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