



CERTSWARRIOR

GIAC GMON

GIAC Continuous Monitoring

Questions&AnswersPDF

ForMoreInformation:

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

Features:

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

Visit us at: <https://www.certswarrior.com/exam/gmon>

Latest Version: 6.0

Question: 1

In device monitoring, what is the purpose of implementing a Security Information and Event Management (SIEM) system?

Response:

- A. To create a physical security barrier around devices.
- B. To provide real-time analysis of security alerts generated by applications and network hardware.
- C. To ensure that all devices use the same operating system.
- D. To increase the processing power of endpoint devices.

Answer: B

Question: 2

For an organization using a federated identity management system, what is a key security advantage?

Response:

- A. Centralized management of all user credentials and permissions.
- B. Decentralized storage of sensitive user data.
- C. Reduced need for multiple user accounts and passwords.
- D. Increased transparency in user activity tracking.

Answer: C

Question: 3

What are effective methods to detect configuration drift in an IT environment?

(Choose Three)

Response:

- A. Manual weekly checks by IT staff.
- B. Automated configuration scanning tools.
- C. Regular user reports on system performance.
- D. Use of a configuration management tool.

Answer: A,B,D

Question: 4

When implementing an access review process, which of the following activities are crucial?

(Choose Two)

Response:

- A. Periodically confirming that user access is still aligned with current roles and responsibilities.
- B. Ensuring that user privileges are expansive to promote ease of use.
- C. Reviewing and adjusting privileges based on user activity and behavior patterns.
- D. Allowing users to modify their own privilege levels to suit their workflow needs.

Answer: A,C

Question: 5

What method is most effective for automatically managing and cycling credentials for privileged accounts?

(Choose Three)

Response:

- A. Manual rotation by system administrators.
- B. Automated privileged identity management solutions.
- C. Using a single, strong static password for all accounts.
- D. Implementation of a privileged access management (PAM) tool.

Answer: A,B,D

Question: 6

An administrator needs to ensure compliance with a policy that mandates two-factor authentication.

Which of the following scenarios would be compliant?

Response:

- A. A system access using a password and security questions.
- B. A system access using a password and a biometric input.
- C. A system access using a hardware token and a mobile push notification.
- D. A system access using a password only.

Answer: B

Question: 7

Why is maintaining an accurate software inventory crucial for organizational security?

Response:

- A. It ensures software compliance with industry standards.
- B. It helps identify unauthorized software that may pose security risks.
- C. It allows for faster software updates.
- D. It reduces the cost of software licenses.

Answer: B

Question: 8

Which method can improve the detection of encrypted intrusions without decrypting the traffic?

Response:

- A. Relying solely on IP address filtering
- B. Analyzing the timing and size of encrypted packets
- C. Implementing strict firewall rules to block all encrypted traffic
- D. Monitoring only unencrypted traffic

Answer: B

Question: 9

Endpoint discovery typically includes identification of what types of devices?

Response:

- A. Only mobile devices
- B. Workstations, mobile devices, and servers
- C. Only network printers
- D. Only servers

Answer: B

Question: 10

How do NGFWs differ from traditional firewalls in terms of threat intelligence?

Response:

- A. NGFWs cannot integrate with external threat intelligence sources.
- B. NGFWs use static routing protocols only.
- C. NGFWs integrate global threat intelligence to improve threat detection and blocking.
- D. NGFWs focus exclusively on managing internal network policies.

Answer: 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