



CERTSWARRIOR

GIAC GSTRT

GIAC Strategic Planning, Policy, and Leadership (GSTRT)

Questions&AnswersPDF

ForMoreInformation:

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

Features:

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

Latest Version: 6.0

Question: 1

Which of the following is a critical factor when defining security policy enforcement mechanisms?
Response:

- A. Policy complexity
- B. Employee resistance
- C. Availability of automated enforcement tools
- D. Clear communication of the consequences for non-compliance

Answer: D

Question: 2

Your organization has identified a need to update its access control policy to reflect changes in user roles and new compliance requirements. Several departments have raised concerns about the complexity of the updated policy.
How would you ensure the policy update is effectively implemented while addressing these concerns?
Response:

- A. Implement the policy immediately without consultation
- B. Simplify the policy by removing key compliance requirements
- C. Involve department heads in a collaborative review of the policy, provide training sessions to explain the changes, and create documentation that clarifies how the policy affects each department
- D. Delay the policy update until all departments agree

Answer: C

Question: 3

How does benchmarking help in the analysis of a security program?
Response:

- A. It compares the program against industry standards and peers to identify strengths and weaknesses
- B. It reduces the workload of the security team
- C. It eliminates the need for internal audits
- D. It simplifies compliance with regulations

Answer: A

Question: 4

Why is it important to regularly review and update cybersecurity policies?

Response:

- A. To keep the policy brief and limit the number of updates
- B. To adjust the policy to account for new threats, regulations, and business changes
- C. To prevent stakeholders from becoming too familiar with the policy
- D. To remove outdated sections without consulting key stakeholders

Answer: B

Question: 5

What is a common leadership challenge during organizational change in cybersecurity?

Response:

- A. Identifying technical solutions
- B. Managing resistance from team members who are comfortable with existing systems
- C. Setting arbitrary deadlines
- D. Avoiding the technical aspects of the change

Answer: B

Question: 6

You have just taken over as a manager of a cybersecurity team that has been struggling with meeting deadlines due to poor communication. Your initial assessment shows that team members are hesitant to share ideas and provide updates in meetings.

What is the most effective approach to improve communication and team performance?

Response:

- A. Implement a strict reporting structure where all updates go directly to you
- B. Introduce weekly team meetings that include time for idea sharing and feedback, and encourage one-on-one check-ins with team members
- C. Require all communication to be conducted via email and reviewed before meetings
- D. Use an anonymous feedback system for team members to submit ideas without speaking in meetings

Answer: B

Question: 7

When assessing the maturity of a security program, which of the following tools or frameworks is often used?

Response:

- A. ISO 27001
- B. Microsoft Excel
- C. SQL database
- D. Adobe Photoshop

Answer: A

Question: 8

In the context of cybersecurity policy development, what is the purpose of conducting a risk assessment?

Response:

- A. To prioritize technical controls over business goals
- B. To make the policy more complex and comprehensive
- C. To reduce the length of the policy document
- D. To identify potential security risks and ensure that the policy addresses those risks

Answer: D

Question: 9

Which of the following is the first step in developing an effective cybersecurity policy?

Response:

- A. Conducting a threat analysis
- B. Identifying key stakeholders
- C. Drafting the policy document
- D. Selecting security tools

Answer: B

Question: 10

Which type of threat actor is most likely motivated by financial gain?

Response:

- A. Nation-state actors
- B. Hacktivists
- C. Cybercriminals
- D. Insider threats

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