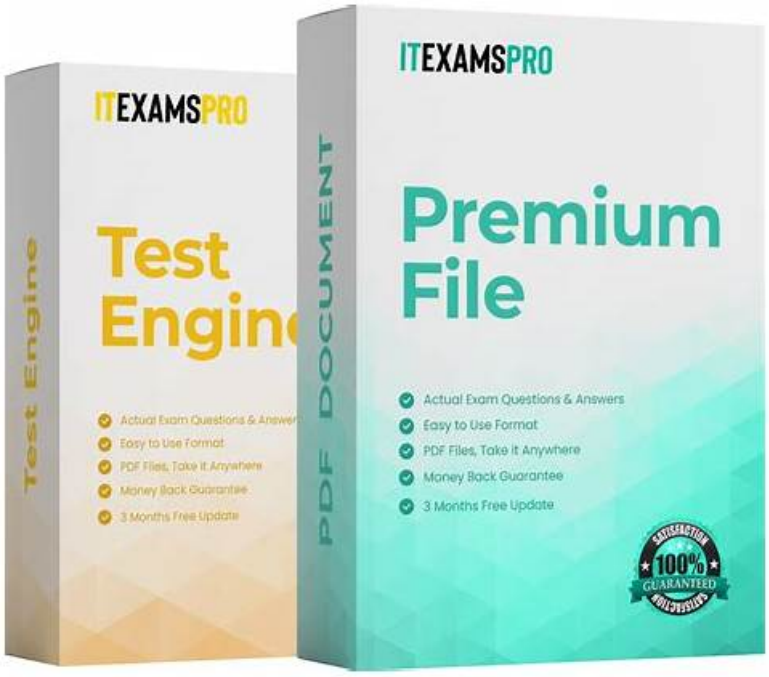
Go With Microsoft GH-500 Exam Dumps [2025] For Instant Success



What's more, part of that TestPDF GH-500 dumps now are free: https://drive.google.com/open?id=1-WwA324RQEuoI7MENZXgKGkPGKltLCGY

You can now get Microsoft GH-500 exam certification our TestPDF have the full version of Microsoft GH-500 exam. You do not need to look around for the latest Microsoft GH-500 training materials, because you have to find the best Microsoft GH-500 Training Materials. Rest assured that our questions and answers, you will be completely ready for the Microsoft GH-500 certification exam.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• Describe GitHub Advanced Security best practices, results, and how to take corrective measures: This section evaluates skills of Security Managers and Development Team Leads in effectively handling GHAS results and applying best practices. It includes using Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) identifiers to describe alerts and suggest remediation, decision-making processes for closing or dismissing alerts including documentation and data-based decisions, understanding default CodeQL query suites, how CodeQL analyzes compiled versus interpreted languages, the roles and responsibilities of development and security teams in workflows, adjusting severity thresholds for code scanning pull request status checks, prioritizing secret scanning remediation with filters, enforcing CodeQL and Dependency Review workflows via repository rulesets, and configuring code scanning, secret scanning, and dependency analysis to detect and remediate vulnerabilities earlier in the development lifecycle, such as during pull requests or by enabling push protection.

Topic 2	• Describe the GHAS security features and functionality: This section of the exam measures skills of Security Engineers and Software Developers and covers understanding the role of GitHub Advanced Security (GHAS) features within the overall security ecosystem. Candidates learn to differentiate security features available automatically for open source projects versus those unlocked when GHAS is paired with GitHub Enterprise Cloud (GHEC) or GitHub Enterprise Server (GHES). The domain includes knowledge of Security Overview dashboards, the distinctions between secret scanning and code scanning, and how secret scanning, code scanning, and Dependabot work together to secure the software development lifecycle. It also covers scenarios contrasting isolated security reviews with integrated security throughout the development lifecycle, how vulnerable dependencies are detected using manifests and vulnerability databases, appropriate responses to alerts, the risks of ignoring alerts, developer responsibilities for alerts, access management for viewing alerts, and the placement of Dependabot alerts in the development process.
Topic 3	• Configure and use secret scanning: This domain targets DevOps Engineers and Security Analysts with the skills to configure and manage secret scanning. It includes understanding what secret scanning is and its push protection capability to prevent secret leaks. Candidates differentiate secret scanning availability in public versus private repositories, enable scanning in private repos, and learn how to respond appropriately to alerts. The domain covers alert generation criteria for secrets, user role-based alert visibility and notification, customizing default scanning behavior, assigning alert recipients beyond admins, excluding files from scans, and enabling custom secret scanning within repositories.
Topic 4	• Configure and use Code Scanning with CodeQL: This domain measures skills of Application Security Analysts and DevSecOps Engineers in code scanning using both CodeQL and third-party tools. It covers enabling code scanning, the role of code scanning in the development lifecycle, differences between enabling CodeQL versus third-party analysis, implementing CodeQL in GitHub Actions workflows versus other CI tools, uploading SARIF results, configuring workflow frequency and triggering events, editing workflow templates for active repositories, viewing CodeQL scan results, troubleshooting workflow failures and customizing configurations, analyzing data flows through code, interpreting code scanning alerts with linked documentation, deciding when to dismiss alerts, understanding CodeQL limitations related to compilation and language support, and defining SARIF categories.
Topic 5	• Configure and use Dependabot and Dependency Review: Focused on Software Engineers and Vulnerability Management Specialists, this section describes tools for managing vulnerabilities in dependencies. Candidates learn about the dependency graph and how it is generated, the concept and format of the Software Bill of Materials (SBOM), definitions of dependency vulnerabilities, Dependabot alerts and security updates, and Dependency Review functionality. It covers how alerts are generated based on the dependency graph and GitHub Advisory Database, differences between Dependabot and Dependency Review, enabling and configuring these tools in private repositories and organizations, default alert settings, required permissions, creating Dependabot configuration files and rules to auto-dismiss alerts, setting up Dependency Review workflows including license checks and severity thresholds, configuring notifications, identifying vulnerabilities from alerts and pull requests, enabling security updates, and taking remediation actions including testing and merging pull requests.

GH-500 Download Free Dumps - GH-500 Valid Exam Testking

If you are going to purchase GH-500 test materials online, the safety of the website is significant. We provide you with a clean and safe online shopping environment if you buying GH-500 trining materials form us. We have professional technicians to exam the website every day, therefore the safety for the website can be guaranteed. Moreover, GH-500 Exam Materials are high quality and accuracy, and you can pass the exam just one time. We offer you free update for 356 days for GH-500 traing materials and the update version will be sent to your email automatically.

Microsoft GitHub Advanced Security Sample Questions (Q45-Q50):

NEW QUESTION # 45

What is the first step you should take to fix an alert in secret scanning?

- A. Archive the repository.
- B. Update your dependencies.
- C. Remove the secret in a commit to the main branch.
- D. Revoke the alert if the secret is still valid.

Answer: D

Explanation:
The first step when you receive a secret scanning alert is to revoke the secret if it is still valid. This ensures the secret can no longer be used maliciously. Only after revoking it should you proceed to remove it from the code history and apply other mitigation steps. Simply deleting the secret from the code does not remove the risk if it hasn't been revoked - especially since it may already be exposed in commit history.

NEW QUESTION # 46
Which of the following statements best describes secret scanning push protection?

- A. Secret scanning alerts must be closed before a branch can be merged into the repository.
- B. Commits that contain secrets are blocked before code is added to the repository.
- C. Buttons for sensitive actions in the GitHub UI are disabled.
- D. Users need to reply to a 2FA challenge before any push events.

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
Secret scanning push protection is a proactive feature that scans for secrets in your code during the push process. If a secret is detected, the push is blocked, preventing the secret from being added to the repository. This helps prevent accidental exposure of sensitive information.
GitHub Docs

NEW QUESTION # 47
After investigating a code scanning alert related to injection, you determine that the input is properly sanitized using custom logic. What should be your next step?

- A. Open an issue in the CodeQL repository.
- B. Draft a pull request to update the open-source query.
- C. Ignore the alert.
- D. Dismiss the alert with the reason "false positive."

Answer: D

Explanation:
When you identify that a code scanning alert is a false positive-such as when your code uses a custom sanitization method not recognized by the analysis-you should dismiss the alert with the reason "false positive." This action helps improve the accuracy of future analyses and maintains the relevance of your security alerts.
As per GitHub's documentation:
"If you dismiss a CodeQL alert as a false positive result, for example because the code uses a sanitization library that isn't supported, consider contributing to the CodeQL repository and improving the analysis." By dismissing the alert appropriately, you ensure that your codebase's security alerts remain actionable and relevant.

NEW QUESTION # 48
Where can you find a deleted line of code that contained a secret value?

- A. Insights
- B. Issues
- C. Commits

- D. Dependency graph

Answer: C

Explanation:
Secrets committed and then deleted are still accessible in the repository's Git history. To locate them, navigate to the Commits tab. GitHub's secret scanning can detect secrets in both current and historical commits, which is why remediation should also include revoking the secret, not just removing it from the latest code.

NEW QUESTION # 49
Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

- A. A user who has write access to the repository
- B. A user who has read access to the repository
- C. A repository member of an enterprise organization
- D. An enterprise administrator

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.
Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.

NEW QUESTION # 50
.....

www.examcollectionpass.com ” and search for ➽ GH-500 □ to obtain a free download □GH-500 Demo Test

- chaceacademy.com, ncon.edu.sa, patersontemple.com, dougwar742.jiliblog.com, myportal.utt.edu.tt, ezupsc.com, darussalamonline.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes