Free PDF Quiz 2026 Microsoft Latest GH-500: GitHub Advanced Security Exam Passing Score

What's more, part of that Getcertkey GH-500 dumps now are free: https://drive.google.com/open?id=1SSBaYgme8yGERNS36z7023Rqz4rbc6ZG

In order to make the GH-500 exam easier for every candidate, Getcertkey compiled such a wonderful GH-500 study materials that allows making you test and review history performance, and then you can find your obstacles and overcome them. In addition, once you have used this type of GH-500 Exam Question online for one time, next time you can practice in an offline environment. It must be highest efficiently exam tool to help you pass the GH-500 exam.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 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 Study Questions - GH-500 Free Demo & GH-500 Valid Torrent

When you see other people in different industry who feel relaxed with high salary, do you want to try another field? And is the difficulty of learning a new piece of knowledge often deterring you? It doesn't matter, now GH-500 practice exam offers you a great opportunity to enter a new industry. Our GH-500 learning material was compiled from the wisdom and sweat of many industry experts. And it is easy to learn and understand our GH-500 exam questions.

Microsoft GitHub Advanced Security Sample Questions (Q68-Q73):

NEW QUESTION # 68
What combination of security measures helps to mitigate risks throughout the SDLC (Software Development Life Cycle)?

- A. View alerts about dependencies that are known to contain security vulnerabilities
- B. Automatically raise pull requests, which reduces your exposure to older versions of dependencies
- C. Confidentially report security vulnerabilities and privately discuss and fix security vulnerabilities in your repository's code
- D. Search for potential security vulnerabilities, detect secrets, and show the full impact of changes to dependencies

Answer: D

Explanation:
These three features provide a complete layer of defense:
Code scanning identifies security flaws in your source code
Secret scanning detects exposed credentials
Dependency review shows the impact of package changes during a pull request Together, they give developers actionable insight into risk and coverage throughout the SDLC.

NEW QUESTION # 69
Where can you find a deleted line of code that contained a secret value?

- A. Insights
- B. Issues
- C. Dependency graph
- D. Commits

Answer: D

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 # 70
What is a security policy?

- A. A file in a GitHub repository that provides instructions to users about how to report a security vulnerability
- B. An alert about dependencies that are known to contain security vulnerabilities
- C. An automatic detection of security vulnerabilities and coding errors in new or modified code
- D. A security alert issued to a community in response to a vulnerability

Answer: A

Explanation:
A security policy is defined by a SECURITY.md file in the root of your repository or .github/ directory. This file informs contributors and security researchers about how to responsibly report vulnerabilities. It improves your project's transparency and ensures timely communication and mitigation of any reported issues.
Adding this file also enables a "Report a vulnerability" button in the repository's Security tab.

NEW QUESTION # 71
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

- A. trigger
- B. commit
- C. pull_request
- D. workflow_dispatch

Answer: C,D

Explanation:
Comprehensive and Detailed Explanation:
Dependency review is triggered by specific events in GitHub workflows:
pull_request: When a pull request is opened, synchronized, or reopened, GitHub can analyze the changes in dependencies and provide a dependency review.
workflow_dispatch: This manual trigger allows users to initiate workflows, including those that perform dependency reviews.
The trigger and commit options are not recognized GitHub Actions events and would not initiate a dependency review.

NEW QUESTION # 72
What are Dependabot security updates?

- A. Automated pull requests to update the manifest to the latest version of the dependency
- B. Automated pull requests that help you update dependencies that have known vulnerabilities
- C. Automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities
- D. Compatibility scores to let you know whether updating a dependency could cause breaking changes to your project

Answer: B

Explanation:
Dependabot security updates are automated pull requests triggered when GitHub detects a vulnerability in a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to the minimum safe version that fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

NEW QUESTION # 73
.....

With the rapid development of the economy, the demands of society on us are getting higher and higher. If you can have GH-500 certification, then you will be more competitive in society. We have chosen a large number of professionals to make GH-500 learning question more professional, while allowing our study materials to keep up with the times. Of course, we do it all for you to get the information you want, and you can make faster progress. You can also get help from GH-500 Exam Training professionals at any time when you encounter any problems. We can be sure that with the professional help of our GH-500 test guide you will surely get a very good experience. Good materials and methods can help you to do more with less. Choose GH-500 test guide to get you closer to success.