Free PDF Quiz Microsoft - GH-500 - Unparalleled GitHub Advanced Security Visual Cert Exam

BTW, DOWNLOAD part of Fast2test GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=10WTFoOi1qHxt5DD8QgMjGx2hjt1kS_kv

Fast2test not only provides you with the best Microsoft practice exam materials, but also with the most comprehensive service. If you buy our GH-500 exam questions and answers, you can get the right of free update exam pdf one-year. And you can try the free demo of our braindumps before you decide to buy. You will pass GH-500 Exam Tests with the help of our latest learning materials and top questions.

You can customize GH-500 exam questions complexity levels and test duration during any attempt. Real Microsoft GH-500 practice test questions like scenarios that the online test creates will enable you to control anxiety. Self-evaluation reports of the GH-500 web-based practice test will inform you where you exactly stand before the final Microsoft GH-500 test. GH-500 Exam Questions in this Microsoft GH-500 practice test are similar to the real test.

>> GH-500 Visual Cert Exam <<

GH-500 Real Exam - GH-500 Braindump Free

If you are busy with your work and have little time to prepare for the exam. You can just choose our GH-500 learning materials, and you will save your time. You just need to spend about 48 to 72 hours on practicing, and you can pass the exam successfully. GH-500 exam materials are edited by professional experts, therefore they are high-quality. And GH-500 Learning Materials of us also have certain quantity, and they will be enough for you to carry on practice. We offer you free demo for you to try before buying GH-500 exam dumps, so that you can know the format of the complete version.

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	• 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 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 4	• 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.
Topic 5	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q114-Q119):

NEW QUESTION # 114
Which of the following features can be used to enforce passing status checks for code scanning and dependency review workflows?

- A. status enforcement
- B. Insights
- C. security GuardRails
- D. repository rulesets

Answer: D

NEW QUESTION # 115
You are configuring a CodeQL workflow for compiled languages. What happens if your workflow uses a language matrix?

- A. Autobuild attempts to build each of the languages listed in the matrix.
- B. Autobuild attempts to build the supported language that has the most source files in the repository.
- C. You may need to install additional software to use the autobuild process.
- D. Analysis of other languages in your repository will fail unless you supply explicit build commands.

Answer: A

Explanation:
If your workflow uses a language matrix, autobuild attempts to build each of the compiled languages listed in the matrix. Without a matrix autobuild attempts to build the supported compiled language that has the most source files in the repository. With the exception of Go, analysis of other compiled languages in your repository will fail unless you supply explicit build commands.
Note:
CodeQL build modes
The CodeQL action supports three different build modes for compiled languages:
none - the CodeQL database is created directly from the codebase without building the codebase (supported for all interpreted languages, and additionally supported for C/C++, C# and Java).
autobuild - CodeQL detects the most likely build method and uses this to attempt to build the codebase and create a database for analysis (supported for all compiled languages).
manual - you define the build steps to use for the codebase in the workflow (supported for all compiled languages, except Rust).

NEW QUESTION # 116
Which of the following pre-defined roles is required to manage code scanning alerts in a repository?

- A. Maintain
- B. Triage
- C. View
- D. Read

Answer: D

Explanation:
Access requirements for security features
In this section, you can find the access required for security features, such as GitHub Advanced Security features.
Note: Repository roles for organizations
You can give organization members, outside collaborators, and teams of people different levels of access to repositories owned by an organization by assigning them to roles. Choose the role that best fits each person or team's function in your project without giving people more access to the project than they need.
From least access to most access, the roles for an organization repository are:
Read: Recommended for non-code contributors who want to view or discuss your project Triage: Recommended for contributors who need to proactively manage issues, discussions, and pull requests without write access Write: Recommended for contributors who actively push to your project Maintain: Recommended for project managers who need to manage the repository without access to sensitive or destructive actions Admin: Recommended for people who need full access to the project, including sensitive and destructive actions like managing security or deleting a repository

NEW QUESTION # 117
Which of the following benefits do code scanning, secret scanning, and dependency review provide?

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

Answer: D

NEW QUESTION # 118
What is the first step you should take to fix an alert in secret scanning?

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

Answer: A

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 # 119
......

P.S. Free 2026 Microsoft GH-500 dumps are available on Google Drive shared by Fast2test: https://drive.google.com/open?id=10WTFoOi1qHxt5DD8QgMjGx2hjt1kS_kv