100% Pass Quiz Newest Microsoft - GH-500 - Valid GitHub Advanced Security Test Review

2026 Latest PDFVCE GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1WBW_PTyQEdaNSou6WlYLzioWY6VwQhUb

PDFVCE's GH-500 exam certification training materials include GH-500 exam dumps and answers. The data is worked out by our experienced team and IT professionals through their own exploration and continuous practice, and its authority is unquestioned. You can download GH-500 free demo and answers on probation on PDFVCE website. After you purchase GH-500 exam certification training information, we will provide one year free renewal service.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 5	• 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.

Precise GH-500 Exam Questions offer you high-efficient Study Materials - PDFVCE

Our GH-500 practice test software contains multiple learning tools that will help you pass the GitHub Advanced Security in the first attempt. We provide actual GH-500 questions pdf dumps also for quick practice. Our GH-500 vce products are easy to use, and you can simply turn things around by going through all the GitHub Advanced Security exam material to ensure your success in the exam. Our GH-500 Pdf Dumps will help you prepare for the GitHub Advanced Security even when you are at work.

Microsoft GitHub Advanced Security Sample Questions (Q82-Q87):

NEW QUESTION # 82
As a repository owner, you do not want to run a GitHub Actions workflow when changes are made to any .txt or markdown files. How would you adjust the event trigger for a pull request that targets the main branch? Each answer presents part of the solution. (Choose three.)
1. on:
2. push:
3. branches: [main, protected]
4. pull_request:
5. branches: [main]

- A. - '**/*.md'

- B. paths-ignore:
- C. - '*/docs/*.md'
- D. paths:
- E. - '**/*.txt'

Answer: A,B,E

Explanation:
[A, not B, D] Use the paths filter when you want to include file path patterns or when you want to both include and exclude file path patterns. Use the paths-ignore filter when you only want to exclude file path patterns. You cannot use both the paths and paths-ignore filters for the same event in a workflow.
[Not E] Pattern: docs/**/*.md
A file with a .md suffix anywhere in the docs directory.

NEW QUESTION # 83
If default code security settings have not been changed at the repository, organization, or enterprise level, which repositories receive Dependabot alerts?

- A. None
- B. Repositories owned by an organization
- C. Repositories owned by an enterprise account
- D. Private repositories

Answer: A

Explanation:
By default, no repositories receive Dependabot alerts unless configuration is explicitly enabled. GitHub does not enable Dependabot alerts automatically for any repositories unless:
The feature is turned on manually
It's configured at the organization or enterprise level via security policies This includes public, private, and enterprise-owned repositories - manual activation is required.

NEW QUESTION # 84
When code scanning is enabled, what is one default event that triggers a scan?

- A. Creating a new branch.
- B. Pushing a change.
- C. Merging a branch.
- D. Deleting a branch.

Answer: B

NEW QUESTION # 85
Which of the following would raise secret scanning alerts?

- A. server-side request forgery
- B. structured query language (SQL) injection
- C. cross site scripting (XSS)
- D. GitHub personal access token

Answer: D

Explanation:
A secret scanning alert is raised when sensitive data, such as API keys, passwords, or access tokens, is detected in a code repository, often due to accidental inclusion by developers. The detection uses pattern-matching and entropy analysis to identify high-entropy strings that look like secrets, but can sometimes generate false positives from non-sensitive data like UUIDs. Alerts can also occur when a developer attempts to bypass the push protection feature that prevents secrets from being committed.

NEW QUESTION # 86
What is a prerequisite to define a custom pattern for a repository?

- A. Change the repository visibility to Internal
- B. Specify additional match criteria
- C. Enable secret scanning
- D. Close other secret scanning alerts

Answer: C

Explanation:
You must enable secret scanning before defining custom patterns. Secret scanning provides the foundational capability for detecting exposed credentials, and custom patterns build upon that by allowing organizations to specify their own regex-based patterns for secrets unique to their environment.
Without enabling secret scanning, GitHub will not process or apply custom patterns.

NEW QUESTION # 87
.....