GH-500 Detail Explanation, GH-500 Valid Braindumps Ebook

P.S. Free 2026 Microsoft GH-500 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1zoy0dCYh8sVsC5S5X_14-3M2j1J43Hwv

To keep with the fast-pace social life, we provide the fastest delivery services on our GH-500 exam questions. As most of the people tend to use express delivery to save time, our GH-500 preparation exam will be sent out within 5-10 minutes after purchasing. As long as you pay at our platform, we will deliver the relevant GH-500 Exam Materials to your mailbox within the given time. Our company attaches great importance to overall services, if there is any problem about the delivery of GH-500 exam materials, please let us know, a message or an email will be available.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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	• 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.

GH-500 Valid Braindumps Ebook, GH-500 Online Test

TestKingIT Microsoft GH-500 practice exam support team cooperates with users to tie up any issues with the correct equipment. If GitHub Advanced Security (GH-500) certification exam material changes, TestKingIT also issues updates free of charge for 1 year following the purchase of our GitHub Advanced Security (GH-500) exam questions.

Microsoft GitHub Advanced Security Sample Questions (Q40-Q45):

NEW QUESTION # 40
Which CodeQL query suite provides queries of lower severity than the default query suite?

- A. github/codeql-go/ql/src@main
- B. github/codeql/cpp/ql/src@main
- C. security-extended

Answer: C

Explanation:
The security-extended query suite includes additional CodeQL queries that detect lower severity issues than those in the default security-and-quality suite.
It's often used when projects want broader visibility into code hygiene and potential weak spots beyond critical vulnerabilities.
The other options listed are paths to language packs, not query suites themselves.

NEW QUESTION # 41
In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

- A. Add Dependabot rules.
- B. Add a workflow with the dependency review action.
- C. Enable Dependabot security updates.
- D. Enable Dependabot alerts.

Answer: B

Explanation:
You can use the dependency review action to help enforce dependency reviews on pull requests in your repository. The dependency review action scans your pull requests for dependency changes and raises an error if any new dependencies have known vulnerabilities.
Note: About dependency review
Dependency review helps you understand dependency changes and the security impact of these changes at every pull request. It provides an easily understandable visualization of dependency changes with a rich diff on the "Files Changed" tab of a pull request.
Dependency review informs you of:
Which dependencies were added, removed, or updated, along with the release dates How many projects use these components Vulnerability data for these dependencies Dependency review allows you to "shift left". You can use the provided predictive information to catch vulnerable dependencies before they hit production.

NEW QUESTION # 42
Which of the following is the most proactive and practical way to prevent new secret scanning alerts?

- A. Enable push protection.
- B. Use feature branches
- C. Scan for non-provider patterns
- D. Configure a secret scanning Actions workflow.

Answer: A

Explanation:
To prevent new secret scanning alerts, enable push protection to block secrets from being committed in the first place, and manage push protection patterns to disable blocking for specific, low-risk secret types or false positives.
Enable Push Protection
Prevent new commits: Push protection proactively scans code for secrets before they are pushed to a repository. If a secret is detected, the push is blocked, providing immediate feedback to developers and preventing secrets from entering the codebase.
Configure patterns: You can configure which secret patterns are blocked at the organization or enterprise level. By disabling patterns that frequently generate false positives, you can reduce the number of new alerts.

NEW QUESTION # 43
By default, where will secret scanning look in a repository in order to execute its job? Each correct answer presents part of the solution. (Choose three.)

- A. full commit history
- B. dependencies
- C. selected files in the repository
- D. all branches
- E. all files in the repository

Answer: A,C,D

Explanation:
Secret scanning scans your entire Git history[D] on all branches [E] present in your GitHub repository for secrets, even if the repository is archived. GitHub will also periodically run a full Git history scan for new secret types in existing content in public repositories where secret scanning is enabled [C, not A] when new supported secret types are added.
Additionally, secret scanning scans:

Descriptions and comments in issues
Titles, descriptions, and comments, in open and closed historical issues. A notification is sent to the relevant partner when a historical partner pattern is detected.
Titles, descriptions, and comments in pull requests
Titles, descriptions, and comments in GitHub Discussions Wikis

NEW QUESTION # 44
When does Dependabot alert you of a vulnerability in your software development process?

- A. when Dependabot opens a pull request to update a vulnerable dependency
- B. when a pull request adding a vulnerable dependency is opened
- C. as soon as a vulnerable dependency is detected
- D. as soon as a pull request is opened by a contributor

Answer: C

Explanation:
Dependabot alerts are generated as soon as GitHub detects a known vulnerability in one of your dependencies. GitHub does this by analyzing your repository's dependency graph and matching it against vulnerabilities listed in the GitHub Advisory Database. Once a match is found, the system raises an alert automatically without waiting for a PR or manual action.
This allows organizations to proactively mitigate vulnerabilities as early as possible, based on real-time detection.

NEW QUESTION # 45
.....

Here in this Desktop practice test software, the GitHub Advanced Security (GH-500) practice questions given are very relevant to the actual GitHub Advanced Security (GH-500) exam. It is compatible with Windows computers. TestKingIT provides its valued customers with customizable GitHub Advanced Security (GH-500) practice exam sessions. The GitHub Advanced Security (GH-500) practice test software also keeps track of the previous Microsoft GH-500 practice exam attempts.

www.stes.tyc.edu.tw, dl.instructure.com, skillboostplatform.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, myportal.utt.edu.tt, poppyksbz245668.blogtov.com, Disposable vapes

P.S. Free 2026 Microsoft GH-500 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1zoy0dCYh8sVsC5S5X_14-3M2j1J43Hwv