Free PDF Efficient Microsoft - GH-500 Exam Quiz

In order to make sure your whole experience of buying our GH-500 prep guide more comfortable, our company will provide all people with 24 hours online service. The experts and professors from our company designed the online service system on our GH-500 exam questions for all customers. If you purchasing the GH-500 Test Practice files designed by many experts and professors from our company, we can promise that our online workers are going to serve you day and night during your learning period. And you can enjoy updates of GH-500 learning guide for one year after purchase.

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	• 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 3	• 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 4	• 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 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 Exam Quiz <<

Microsoft GH-500 Free Demo

Now, let us show you why our GH-500 exam questions are absolutely your good option. First of all, in accordance to the fast-pace changes of bank market, we follow the trend and provide the latest version of GH-500 study materials to make sure you learn more knowledge. Secondly, since our GH-500 training quiz appeared on the market, seldom do we have the cases of customer information disclosure. We really do a great job in this career!

Microsoft GitHub Advanced Security Sample Questions (Q69-Q74):

NEW QUESTION # 69
In a private repository, what minimum requirements does GitHub need to generate a dependency graph? (Each answer presents part of the solution. Choose two.)

- A. Dependency graph enabled at the organization level for all new private repositories
- B. Write access to the dependency manifest and lock files for an enterprise
- C. Read-only access to all the repository's files
- D. Read-only access to the dependency manifest and lock files for a repository

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation:
To generate a dependency graph for a private repository, GitHub requires:
Dependency graph enabled: The repository must have the dependency graph feature enabled. This can be configured at the organization level to apply to all new private repositories.
Access to manifest and lock files: GitHub needs read-only access to the repository's dependency manifest and lock files (e.g., package.json, requirements.txt) to identify and map dependencies.

NEW QUESTION # 70
Secret scanning will scan:

- A. Any Git repository.
- B. External services.
- C. A continuous integration system.
- D. The GitHub repository.

Answer: D

Explanation:
Secret scanning is a feature provided by GitHub that scans the contents of your GitHub repositories for known types of secrets, such as API keys and tokens. It operates within the GitHub environment and does not scan external systems, services, or repositories outside of GitHub. Its primary function is to prevent the accidental exposure of sensitive information within your GitHub-hosted code.

NEW QUESTION # 71
Which of the following Watch settings could you use to get Dependabot alert notifications? (Each answer presents part of the solution. Choose two.)

- A. The All Activity setting
- B. The Participating and @mentions setting
- C. The Ignore setting
- D. The Custom setting

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation:
To receive Dependabot alert notifications for a repository, you can utilize the following Watch settings:
Custom setting: Allows you to tailor your notifications, enabling you to subscribe specifically to security alerts, including those from Dependabot.
All Activity setting: Subscribes you to all notifications for the repository, encompassing issues, pull requests, and security alerts like those from Dependabot.
The Participating and @mentions setting limits notifications to conversations you're directly involved in or mentioned, which may not include security alerts. The Ignore setting unsubscribes you from all notifications, including critical security alerts.
GitHub Docs
+1
GitHub Docs
+1

NEW QUESTION # 72
Assuming security and analysis features are not configured at the repository, organization, or enterprise level, secret scanning is enabled on:

- A. Public repositories
- B. User-owned private repositories
- C. Private repositories

- D. All new repositories within your organization

Answer: A

Explanation:
By default, secret scanning is enabled automatically for all public repositories. For private or internal repositories, secret scanning must be enabled manually unless configured at the organization or enterprise level.
This default behavior helps protect open-source projects without requiring additional configuration.

NEW QUESTION # 73
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 # 74
......

Web-based GitHub Advanced Security (GH-500) practice test of VCE4Plus is accessible from any place. You merely need an active internet connection to take this Microsoft GH-500 practice exam. Browsers including MS Edge, Internet Explorer, Safari, Opera, Chrome, and Firefox support this GitHub Advanced Security (GH-500) practice exam. Additionally, this GitHub Advanced Security (GH-500) test is supported by operating systems including Android, Mac, iOS, Windows, and Linux.

Latest GH-500 Test Simulator: https://www.vce4plus.com/Microsoft/GH-500-valid-vce-dumps.html

www.stes.tyc.edu.tw, bijie.cnrxw.cn, 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, www.cncircus.com.cn, demo.webdive.in, muketm.cn, 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, Disposable vapes

P.S. Free 2026 Microsoft GH-500 dumps are available on Google Drive shared by VCE4Plus: https://drive.google.com/open?id=1DvEYWjVf7U_tYhbKkYcPMQOCniA44R8S