2025 GH-500 Pass4sure - GitHub Advanced Security Realistic New Test Testking Free PDF

You can free download part of BraindumpsIT's practice questions and answers about Microsoft certification GH-500 exam online, as an attempt to test our quality. As long as you choose to purchase BraindumpsIT's products, we will do our best to help you pass Microsoft Certification GH-500 Exam disposably.

BraindumpsIT have the obligation to ensure your comfortable learning if you have spent money on our GH-500 study materials. We do not have hot lines. The pass rate of our GH-500 is as high as more then 98%. And you can enjoy our considerable service on GH-500 exam questions. So you are advised to send your emails to our email address. In case you send it to others' email inbox, please check the address carefully before. The after-sales service of website can stand the test of practice. Once you trust our GH-500 Exam Torrent, you also can enjoy such good service.

>> GH-500 Pass4sure <<

Get Authoritative GH-500 Pass4sure and Useful New GH-500 Test Testking

After you visit the pages of our GH-500 test torrent on the websites, you can know the version of the product, the updated time, the quantity of the questions and answers, the characteristics and merits of the GitHub Advanced Security guide torrent, the price of the product and the discounts. In the pages of our product on the website, you can find the details and guarantee and the contact method, the evaluations of the client on our GH-500 Test Torrent and other information about our product. So it is very convenient for you.

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 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 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 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.

Microsoft GitHub Advanced Security Sample Questions (Q11-Q16):

NEW QUESTION # 11
Where can you use CodeQL analysis for code scanning? (Each answer presents part of the solution. Choose two.)

- A. In a workflow
- B. In an external continuous integration (CI) system
- C. In the Files changed tab of the pull request
- D. In a third-party Git repository

Answer: A,B

Explanation:
In a workflow: GitHub Actions workflows are the most common place for CodeQL code scanning. The codeql-analysis.yml defines how the analysis runs and when it triggers.
In an external CI system: GitHub allows you to run CodeQL analysis outside of GitHub Actions. Once complete, the results can be uploaded using the upload-sarif action to make alerts visible in the repository.
You cannot run or trigger analysis from third-party repositories directly, and the Files changed tab in pull requests only shows diff - not analysis results.

NEW QUESTION # 12
Assuming there is no custom Dependabot behavior configured, where possible, what does Dependabot do after sending an alert about a vulnerable dependency in a repository?

- A. Scans repositories for vulnerable dependencies on a schedule and adds those files to a manifest
- B. Constructs a graph of all the repository's dependencies and public dependents for the default branch
- C. Creates a pull request to upgrade the vulnerable dependency to the minimum possible secure version
- D. Scans any push to all branches and generates an alert for each vulnerable repository

Answer: C

Explanation:
After generating an alert for a vulnerable dependency, Dependabot automatically attempts to create a pull request to upgrade that dependency to the minimum required secure version-if a fix is available and compatible with your project.
This automated PR helps teams fix vulnerabilities quickly with minimal manual intervention. You can also configure update behaviors using dependabot.yml, but in the default state, PR creation is automatic.

NEW QUESTION # 13
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

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

Answer: A,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 # 14
In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

- A. Add a workflow with the dependency review action.

- B. Enable Dependabot security updates.
- C. Enable Dependabot alerts.
- D. Add Dependabot rules.

Answer: A

Explanation:
To detect and block vulnerable dependencies before merge, developers should use the Dependency Review GitHub Action in their pull request workflows. It scans all proposed dependency changes and flags any packages with known vulnerabilities.
This is a preventative measure during development, unlike Dependabot, which reacts after the fact.

NEW QUESTION # 15
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 # 16
......

When you click into BraindumpsIT's site, you will see so many people daily enter the website. You can not help but be surprised. In fact, this is normal. BraindumpsIT is provide different training materials for alot of candidates. They are using our training materials tto pass the exam. This shows that our Microsoft GH-500 Exam Training materials can really play a role. If you want to buy, then do not miss BraindumpsIT website, you will be very satisfied.

New GH-500 Test Testking: https://www.braindumpsit.com/GH-500_real-exam.html

- GH-500 Excellect Pass Rate □ New GH-500 Exam Topics □ GH-500 Valid Exam Vce □ Open ▹ www.torrentvce.com ◃ enter □ GH-500 □ and obtain a free download □Latest GH-500 Exam Simulator
- Helpful Features of GH-500 PDF Questions □ Search on [www.pdfvce.com] for □ GH-500 □ to obtain exam materials for free download □New GH-500 Exam Simulator
- Download www.prep4away.com Microsoft GH-500 Exam Dumps and Start Preparation □ Search for ▸ GH-500 ◂ and download exam materials for free through ⇛ www.prep4away.com ⇚ □Exam GH-500 Tests
- Exam GH-500 Overview □ Practice GH-500 Exams Free □ Exam GH-500 Guide □ Search for ▹ GH-500 ◃ and download it for free on ▸ www.pdfvce.com ◂ website □Latest GH-500 Braindumps Free
- Exam GH-500 Guide □ GH-500 Latest Test Prep □ GH-500 Practice Tests □ Search for （ GH-500 ） on □ www.torrentvalid.com □ immediately to obtain a free download □GH-500 Latest Test Prep
- Latest GH-500 Exam Simulator □ GH-500 Exam Demo □ GH-500 Latest Test Prep □ Easily obtain □ GH-500 □ for free download through 「 www.pdfvce.com 」 □Exam GH-500 Overview
- GitHub Advanced Security exam dumps - GH-500 training pdf - GitHub Advanced Security valid torrent □ Open website □ www.exams4collection.com □ and search for ➠ GH-500 □ for free download □Latest GH-500 Exam Simulator
- Helpful Features of GH-500 PDF Questions □ Download ▹ GH-500 ◃ for free by simply searching on { www.pdfvce.com } □New GH-500 Exam Simulator
- Hot GH-500 Pass4sure | Amazing Pass Rate For GH-500: GitHub Advanced Security | Free PDF New GH-500 Test Testking □ Search for ▸ GH-500 ◂ and download exam materials for free through （ www.pass4leader.com ） □Exam Dumps GH-500 Zip
- Exam Dumps GH-500 Zip □ Exam GH-500 Guide □ GH-500 Excellect Pass Rate □ Enter 【 www.pdfvce.com 】 and search for 《 GH-500 》 to download for free □New GH-500 Dumps Book
- GH-500 Latest Exam Format □ New GH-500 Exam Topics □ GH-500 Exam Demo □ Search on ➠

www.torrentvalid.com □ for 「GH-500」 to obtain exam materials for free download □PDF GH-500 Cram Exam

- joyrulez.com, elearning.eauqardho.edu.so, www.stes.tyc.edu.tw, vxlxemito123.blogs-service.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, letterboxd.com, beauhnqrt.blogstival.com, lms.ait.edu.za, Disposable vapes