Microsoft GH-500 Questions–Best Way To Clear The Exam [2026]

What's more, part of that Prep4sureExam GH-500 dumps now are free: https://drive.google.com/open?id=1aBpAo_t8Uus1uHjcAhBcp7LtXjBvD-vR

Prep4sureExam also offers a demo of the Microsoft GH-500 exam product which is absolutely free. Up to 1 year of free GitHub Advanced Security (GH-500) questions updates are also available if in any case the sections of the Microsoft GH-500 actual test changes after your purchase. Lastly, we also offer a full refund guarantee according to terms and conditions if you do not get success in the GitHub Advanced Security Certification Exam after using our GH-500 product. These offers by Prep4sureExam save your time and money. Buy GitHub Advanced Security (GH-500) practice material today.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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 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.

>> GH-500 Reliable Study Notes <<

Valid Microsoft GH-500 Exam Questions | Exam GH-500 Practice

On the basis of the current social background and development prospect, the GH-500 certifications have gradually become accepted prerequisites to stand out the most in the workplace. As far as we know, in the advanced development of electronic technology, lifelong learning has become more accessible, which means everyone has opportunities to achieve their own value and life dream. Our GH-500 Exam Materials are pleased to serve you as such an exam tool. You will have a better future with our GH-500 study braindumps!

Microsoft GitHub Advanced Security Sample Questions (Q59-Q64):

NEW QUESTION # 59
You are a maintainer of a repository and Dependabot notifies you of a vulnerability. Where could the vulnerability have been

disclosed? (Each answer presents part of the solution. Choose two.)

- A. In security advisories reported on GitHub
- B. In the dependency graph
- C. In manifest and lock files
- D. In the National Vulnerability Database

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation:
Dependabot alerts are generated based on data from various sources:
National Vulnerability Database (NVD): A comprehensive repository of known vulnerabilities, which GitHub integrates into its advisory database.
GitHub Docs
Security Advisories Reported on GitHub: GitHub allows maintainers and security researchers to report and discuss vulnerabilities, which are then included in the advisory database.
The dependency graph and manifest/lock files are tools used by GitHub to determine which dependencies are present in a repository but are not sources of vulnerability disclosures themselves.

NEW QUESTION # 60
Where in the repository can you give additional users access to secret scanning alerts?

- A. Insights
- B. Security
- C. Settings
- D. Secrets

Answer: C

Explanation:
To grant specific users access to view and manage secret scanning alerts, you do this via the Settings tab of the repository. From there, under the "Code security and analysis" section, you can add individuals or teams with roles such as security manager.
The Security tab only displays alerts; access control is handled in Settings.

NEW QUESTION # 61
You have enabled security updates for a repository. When does GitHub mark a Dependabot alert as resolved for that repository?

- A. When you merge a pull request that contains a security update
- B. When you dismiss the Dependabot alert
- C. When the pull request checks are successful
- D. When Dependabot creates a pull request to update dependencies

Answer: A

Explanation:
A Dependabot alert is marked as resolved only after the related pull request is merged into the repository. This indicates that the vulnerable dependency has been officially replaced with a secure version in the active codebase.
Simply generating a PR or passing checks does not change the alert status; merging is the key step.

NEW QUESTION # 62
What YAML syntax do you use to exclude certain files from secret scanning?

- A. branches-ignore:
- B. paths-ignore:
- C. decrypt_secret.sh
- D. secret scanning.yml

Answer: B

Explanation:
To exclude specific files or directories from being scanned by secret scanning in GitHub Actions, you can use the paths-ignore: key within your YAML workflow file.
This tells GitHub to ignore specified paths when scanning for secrets, which can be useful for excluding test data or non-sensitive mock content.
Other options listed are invalid:
branches-ignore: excludes branches, not files.
decrypt_secret.sh is not a YAML key.
secret scanning.yml is not a recognized filename for configuration.

NEW QUESTION # 63
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.) on:
pull_request:
branches: [main]

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

Answer: A,B,C

Explanation:
To exclude .txt and .md files from triggering workflows on pull requests to the main branch:
on: defines the event (e.g., pull_request)
pull_request: is the trigger
paths-ignore: is the key used to ignore file patterns
Example YAML:
yaml
CopyEdit
on:
pull_request:
branches:
- main
paths-ignore:
- '*.md'
- '*.txt'
Using paths: would include only specific files instead - not exclude. paths-ignore: is correct here.

NEW QUESTION # 64
......

- Latest GH-500 Exam Materials ⯄ GH-500 Latest Torrent ⯄ GH-500 Certification Book Torrent ⯄ Download ▷ GH-500 ◁ for free by simply searching on ⇒ www.pdfvce.com ⇐ ⯄GH-500 Testing Center
- GH-500 Dumps Questions ⯄ Test GH-500 Engine Version ⯄ GH-500 Latest Torrent ⯄ Search for ⯄ GH-500 ⯄ and easily obtain a free download on ▸ www.testkingpass.com ◂ ⯄Exam GH-500 Passing Score
- Pass Guaranteed Quiz 2026 GH-500: GitHub Advanced Security – Efficient Reliable Study Notes ⯄ Search for ✔ GH-500 ⯄✔ ⯄ and download exam materials for free through 「 www.pdfvce.com 」 ⯄Latest GH-500 Exam Pass4sure
- The Best GH-500 Reliable Study Notes - Reliable Valid GH-500 Exam Questions - Complete Exam GH-500 Practice ⯄ Copy URL 【 www.exam4labs.com 】 open and search for ➥ GH-500 ⯄ to download for free ⯄GH-500 Latest Exam Test
- Test GH-500 Engine Version ⯄ GH-500 Dumps Questions ⯄ Authentic GH-500 Exam Questions ⯄ Open website ⯄ www.pdfvce.com ⯄ and search for ⇒ GH-500 ⇐ for free download ⯄GH-500 Latest Exam Test
- Pass Guaranteed Quiz 2026 Perfect Microsoft GH-500: GitHub Advanced Security Reliable Study Notes ⯄ Open ⯄ www.validtorrent.com ⯄ enter ▸ GH-500 ◂ and obtain a free download ⯄Formal GH-500 Test
- Exam GH-500 Study Guide ⯄ New GH-500 Mock Test ⯄ Exam GH-500 Passing Score ⯄ Immediately open " www.pdfvce.com " and search for ➥ GH-500 ⯄ to obtain a free download ⯄GH-500 Learning Materials
- Microsoft - GH-500 - High Hit-Rate GitHub Advanced Security Reliable Study Notes ⯄ The page for free download of " GH-500 " on ⯄ www.dumpsmaterials.com ⯄ will open immediately ❤ ⯄GH-500 Testing Center
- bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, launchpad.net.in, carrabreconservatoryofmusic.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, Disposable vapes

P.S. Free & New GH-500 dumps are available on Google Drive shared by Prep4sureExam: https://drive.google.com/open?id=1aBpAo_t8Uus1uHjcAhBcp7LtXjBvD-vR