Reliable GH-500 training materials bring you the best GH-500 guide exam: GitHub Advanced Security - ActualTestsQuiz

We try our best to present you the most useful and efficient GH-500 training materials about the test and provide multiple functions and intuitive methods to help the clients learn efficiently. Learning our GH-500 useful test guide costs you little time and energy. The passing rate and hit rate are both high thus you will encounter few obstacles to pass the test. You can further understand our GH-500 study practice guide after you read the introduction on our web.

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 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	• 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 5	• 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.

Dump GH-500 Collection & GH-500 Real Brain Dumps

Perhaps you have had such an unpleasant experience about GH-500 exam questions you brought in the internet was not suitable for you in actual use, to avoid this, our company has prepared GH-500 free demo in this website for our customers, with which you can have your first-hand experience before making your final decision. The content of the free demo is part of the content in our real GH-500 Study Guide. And you can see how excellent our GH-500 training dumps are!

Microsoft GitHub Advanced Security Sample Questions (Q60-Q65):

NEW QUESTION # 60
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

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

Answer: A,B

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 # 61
What do you need to do before you can define a custom pattern for a repository?

- A. Enable secret scanning on the repository.
- B. Add a secret scanning custom pattern.
- C. Provide match requirements for the secret format.
- D. Provide a regular expression for the format of your secret pattern.

Answer: A

Explanation:
Stack Overflow
Explanation:
Comprehensive and Detailed Explanation:
Before defining a custom pattern for secret scanning in a repository, you must enable secret scanning for that repository. Secret scanning must be active to utilize custom patterns, which allow you to define specific formats (using regular expressions) for secrets unique to your organization.
Once secret scanning is enabled, you can add custom patterns to detect and prevent the exposure of sensitive information tailored to your needs.

NEW QUESTION # 62
Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

- A. An enterprise administrator
- B. A user who has write access to the repository
- C. A user who has read access to the repository
- D. A repository member of an enterprise organization

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.
Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.

NEW QUESTION # 63
Which of the following is the best way to prevent developers from adding secrets to the repository?

- A. Create a CODEOWNERS file
- B. Make the repository public
- C. Enable push protection
- D. Configure a security manager

Answer: C

Explanation:
The best proactive control is push protection. It scans for secrets during a git push and blocks the commit before it enters the

repository.
Other options (like CODEOWNERS or security managers) help with oversight but do not prevent secret leaks.
Making a repo public would increase the risk, not reduce it.

NEW QUESTION # 64
In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

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

Answer: B

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 # 65
.....

In the era of informational globalization, the world has witnessed climax of science and technology development, and has enjoyed the prosperity of various scientific blooms. In 21st century, every country had entered the period of talent competition, therefore, we must begin to extend our GH-500 personal skills, only by this can we become the pioneer among our competitors. We here tell you that there is no need to worry about. Our GH-500 Actual Questions are updated in a high speed. Since the date you pay successfully, you will enjoy the GH-500 test guide freely for one year, which can save your time and money. We will send you the latest GH-500 study dumps through your email, so please check your email then.

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.stes.tyc.edu.tw, Disposable vapes