Test Microsoft GH-500 Practice & GH-500 Test Objectives Pdf

BTW, DOWNLOAD part of ExamsTorrent GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=1SZ7Xyb32uu8YITNDXXa1KYB3ga6jR11_

Are you ready to take your career to the next level with the GitHub Advanced Security (GH-500)? Look no further than ExamsTorrent for all of your GH-500 exam needs. Our comprehensive and cost-effective solution includes regularly updated Microsoft GH-500 Exam Questions, available in a convenient PDF format that can be downloaded on any device, including PC, laptop, mac, tablet, and smartphone.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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	• 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.

100% Pass 2026 Efficient Microsoft GH-500: Test GitHub Advanced Security Practice

The social environment is constantly changing, and our GH-500 guide quiz is also advancing with the times. The content of GH-500 exam materials is constantly updated. You can save a lot of time for collecting real-time information. In order to ensure that you can see the updated GH-500 practice prep as soon as possible, our system sends the updated information to your email address first timing. In order to avoid the omission of information, please check your email regularly.

Microsoft GitHub Advanced Security Sample Questions (Q65-Q70):

NEW QUESTION # 65
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. Read-only access to all the repository's files
- C. Write access to the dependency manifest and lock files for an enterprise
- 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 # 66
Which of the following options would close a Dependabot alert?

- A. Viewing the dependency graph
- B. Creating a pull request to resolve the vulnerability that will be approved and merged
- C. Viewing the Dependabot alert on the Dependabot alerts tab of your repository
- D. Leaving the repository in its current state

Answer: B

Explanation:
A Dependabot alert is only marked as resolved when the related vulnerability is no longer present in your code - specifically after you merge a pull request that updates the vulnerable dependency.
Simply viewing alerts or graphs does not affect their status. Ignoring the alert by leaving the repo unchanged keeps the vulnerability active and unresolved.

NEW QUESTION # 67
Which Dependabot configuration fields are required? Each answer presents part of the solution.
(Choose three.)

- A. allow
- B. package-ecosystem
- C. schedule.interval
- D. directory
- E. milestone

Answer: B,C,D

Explanation:
When configuring Dependabot via the dependabot.yml file, the following fields are mandatory for each update configuration:
[D] directory: Specifies the location of the package manifest within the repository. This tellsDependabot where to look for dependency files.
[A] package-ecosystem: Indicates the type of package manager (e.g., npm, pip, maven) used in the specified directory.
[C] schedule.interval: Defines how frequently Dependabot checks for updates (e.g., daily, weekly). This ensures regular scanning for outdated or vulnerable dependencies.
[Not E] The milestone field is optional and used for associating pull requests with milestones. The allow field is also optional and used to specify which dependencies to update.

NEW QUESTION # 68
When secret scanning detects a set of credentials on a public repository, what does GitHub do?

- A. It scans the contents of the commits for additional secrets.
- B. It displays a public alert in the Security tab of the repository.
- C. It notifies the service provider who issued the secret.
- D. It sends a notification to repository members.

Answer: C

Explanation:
When a public repository contains credentials that match known secret formats, GitHub will automatically notify the service provider

that issued the secret. This process is known as "secret scanning partner notification". The provider may then revoke the secret or contact the user directly.
GitHub does not publicly display the alert and does not send internal repository notifications for public detections.

NEW QUESTION # 69
As a repository owner, you want to receive specific notifications, including security alerts, for an individual repository. Which repository notification setting should you use?

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

Answer: C

Explanation:
Using the Custom setting allows you to subscribe to specific event types, such as Dependabot alerts or vulnerability notifications, without being overwhelmed by all repository activity. This is essential for repository maintainers who need fine-grained control over what kinds of events trigger notifications.
This setting is configurable per repository and allows users to stay aware of critical issues while minimizing notification noise.
Note: Configuring your watch settings for an individual repository
You can choose whether to watch or unwatch an individual repository. You can also choose to only be notified of certain event types such as issues, pull requests, releases, security alerts, or discussions (if enabled for the repository), or completely ignore an individual repository.
1.On GitHub, navigate to the main page of the repository.
2. In the upper-right corner, select the "Watch" drop-down menu, then click a watch option.
If you want to further customize notifications, click Custom, then select specific events that you want to be notified of, such as Issues or Pull Requests, in addition to participating and
@mentions.
For example, if you select "Issues", you will be notified about, and subscribed to, updates on every issue (including those that existed prior to you selecting this option) in the repository. If you're @mentioned in a pull request in this repository, you'll receive notifications for that too, and you'll be subscribed to updates on that specific pull request, in addition to being notified about issues.

NEW QUESTION # 70
.....

Owing to the industrious dedication of our experts and other working staff, our GH-500 study materials grow to be more mature and are able to fight against any difficulties. Our GH-500 preparation exam have achieved high pass rate in the industry, and we always maintain a 99% pass rate on our GH-500 Exam Questions with our endless efforts. We have to admit that behind such a starling figure, there embrace mass investments from our company. Since our company's establishment, we have devoted mass manpower, materials and financial resources into GH-500 exam materials.

for ⇛ GH-500 ⇚ on ⇛ www.examcollectionpass.com ⇚ immediately to obtain a free download Test GH-500 Preparation

- Latest GH-500 Exam Cost GH-500 New Braindumps Free Valid Real GH-500 Exam Download ➤ GH-500 for free by simply searching on ➤ www.pdfvce.com GH-500 Pass4sure Dumps Pdf
- Valid Real GH-500 Exam GH-500 Exam Cram Questions GH-500 Latest Test Fee Open website ✔ www.examcollectionpass.com ✔ and search for GH-500 for free download GH-500 Dumps Collection
- GH-500 Dumps Collection Clearer GH-500 Explanation GH-500 Latest Test Fee Simply search for ✔ GH-500 ✔ for free download on ▷ www.pdfvce.com ◁ New GH-500 Exam Bootcamp
- Formal GH-500 Test New GH-500 Exam Bootcamp Test GH-500 Preparation Open website ➡ www.testkingpass.com and search for " GH-500 " for free download Study GH-500 Group
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.zzhan.com.cn, www.stes.tyc.edu.tw, www.mixcloud.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New GH-500 dumps are available on Google Drive shared by ExamsTorrent: https://drive.google.com/open?id=1SZ7Xyb32uu8YITNDXXa1KYB3ga6jR11_