Trustworthy Microsoft GH-500 Exam Content | GH-500 Test Labs

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

The BootcampPDF Microsoft GH-500 exam questions is 100% verified and tested. BootcampPDF Microsoft GH-500 exam practice questions and answers is the practice test software. In BootcampPDF, you will find the best exam preparation material. The material including practice questions and answers. The information we have could give you the opportunity to practice issues, and ultimately achieve your goal that through Microsoft GH-500 Exam Certification.

We provide 3 versions of our GitHub Advanced Security exam torrent and they include PDF version, PC version, APP online version. Each version's functions and using method are different and you can choose the most convenient version which is suitable for your practical situation. For example, the PDF version is convenient for you to download and print our GH-500 test torrent and is suitable for browsing learning. If you use the PDF version you can print our GH-500 Guide Torrent on the papers and it is convenient for you to take notes. You learn our GH-500 test torrent at any time and place. The PC version can stimulate the real exam's environment, is stalled on the Windows operating system and runs on the Java environment. You can use it at any time to test your own exam stimulation tests scores and whether you have mastered our GH-500 guide torrent or not.

>> Trustworthy Microsoft GH-500 Exam Content <<

GH-500 Test Labs - Practice GH-500 Test

Choosing valid Microsoft dumps means closer to success. Before you buy our products, you can download the free demo of GH-500 test questions to check the accuracy of our dumps. Besides, there are 24/7 customer assisting to support you in case you may have any questions about GH-500 Dumps PDF or download link.

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 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 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	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q89-Q94):

NEW QUESTION # 89
Secret scanning will scan:

- A. any Git repository.
- B. a continuous integration system.
- C. external services.
- D. the GitHub repository.

Answer: D

Explanation:
Secret scanning automatically scans your repository's contents for sensitive data, such as API keys, passwords, tokens, and other secrets. It looks for patterns and heuristics that match known types of secrets.
Secret scanning is available for the following repository types:
Public repositories on GitHub.com
Organization-owned repositories on GitHub Team with GitHub Secret Protection enabled

NEW QUESTION # 90
Which of the following is required to block the merge of a pull request containing critical vulnerabilities? Each correct answer presents part of the solution. (Choose two.)

- A. Establish the protection rules in the code security settings.
- B. Add a repository ruleset.
- C. Enable Dependabot for the organization.
- D. Configure a CODEOWNERS file in the repository.

Answer: A,B

Explanation:
Set code scanning merge protection
You can use rulesets to set code scanning merge protection for pull requests.
You can use rulesets to prevent pull requests from being merged when one of the following conditions is met:
A required tool found a code scanning alert of a severity that is defined in a ruleset.
A required code scanning tool's analysis is still in progress.
A required code scanning tool is not configured for the repository.
Note:
Creating a merge protection ruleset for a repository
1. On GitHub, navigate to the main page of the repository.
2. Under your repository name, click Settings. If you cannot see the "Settings" tab, select the dropdown menu, then click Settings.
3. In the left sidebar, under "Code and automation," click Rules, then click Rulesets.
4. Click New ruleset.
5. To create a ruleset targeting branches, click New branch ruleset.
6. Under "Ruleset name," type a name for the ruleset.
7. Optionally, to change the default enforcement status, click Disabled and select an enforcement status.
8. Under "Branch protections", select Require code scanning results.
9. Under "Required tools and alert thresholds", click Add tool and select a code scanning tool with the dropdown. For example, "CodeQL".
10. Next to the name of a code scanning tool:
Click Alerts and select one of: None, Errors, Errors and Warnings or All.
Click Security alerts and select one of: None, Critical, High or higher, Medium or higher, or All.

NEW QUESTION # 91
Assuming that notification and alert recipients are not customized, what does GitHub do when it identifies a vulnerable dependency in a repository where Dependabot alerts are enabled? (Each answer presents part of the solution. Choose two.)

- A. It notifies the repository administrators about the new alert.
- B. It consults with a security service and conducts a thorough vulnerability review.
- C. It generates a Dependabot alert and displays it on the Security tab for the repository.
- D. It generates Dependabot alerts by default for all private repositories.

Answer: A,C

Explanation:
When GitHub identifies a vulnerable dependency in a repository with Dependabot alerts enabled, it performs the following actions:
[A] Geneates a Dependabot alert: The alert is displayed on the repository's Security tab, providing details about the vulnerability and affected dependency.
[D] Notifies repository maintainers: By default, GitHub notifies users with write, maintain, or admin permissions about new Dependabot alerts.
These actions ensure that responsible parties are informed promptly to address the vulnerability.

NEW QUESTION # 92
When does Dependabot alert you of a vulnerability in your software development process?

- A. as soon as a vulnerable dependency is detected
- B. as soon as a pull request is opened by a contributor
- C. when a pull request adding a vulnerable dependency is opened
- D. when Dependabot opens a pull request to update a vulnerable dependency

Answer: A

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 # 93
How does GitHub Advanced Security (GHAS) help integrate security into each step of the software development life cycle?

- A. By generating alerts for outdated dependencies in a project.
- B. By providing access to curated security intelligence from millions of developers and security researchers around the world.
- C. By automating security checks with every pull request, surfacing issues in the context of the development workflow.
- D. By providing a comprehensive dashboard summarizing the security status of the repository.

Answer: C

NEW QUESTION # 94
.....

- Valid Dumps GH-500 Ebook □ Real GH-500 Exams □ Test GH-500 Study Guide □ Open ➽ www.pdfvce.com □ □ and search for ➽ GH-500 □ to download exam materials for free □New GH-500 Dumps
- Obtain Trustworthy GH-500 Exam Content PDF New Version □ Search for [GH-500] and obtain a free download on ⇛ www.torrentvce.com ⇚ □GH-500 Exam Overview
- emiliaempn657627.wikikali.com, 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, rafaelmhkb494625.59bloggers.com, www.stes.tyc.edu.tw, sachintjdl053846.fare-blog.com, 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, p.me-page.com, app.parler.com, jasperanpp381276.tusblogos.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest BootcampPDF GH-500 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1fMNCQm_kQmogfKYQq_mLVNrD-1bSKWpA