Latest Microsoft GH-500 Guide Files - GH-500 Lead2pass

2026 Latest Itcertkey GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1Sl1_icGJFTm0TqBEEFE1wwSCaeEF-ScZ

Itcertkey has designed GH-500 pdf dumps format that is easy to use. Anyone can download Microsoft GH-500 pdf questions file and use it from any location or at any time. Microsoft PDF Questions files can be used on laptops, tablets, and smartphones. Moreover, you will get actual Microsoft GH-500 Exam Questions in this Microsoft GH-500 pdf dumps file.

First and foremost, even though our company has become the staunch force in this field for almost ten years and our GH-500 exam questions have enjoyed such a quick sale in the international market we still keep an affordable price for our customers. Second, we have prepared free demo in this website for our customers to have the first-hand experience of the GH-500 Latest Torrent compiled by our company before making their final decision. So do not hesitate any more, just hurry up to buy our GH-500 test question which will never let you down.

>> Latest Microsoft GH-500 Guide Files <<

100% Pass Quiz Microsoft - Efficient GH-500 - Latest GitHub Advanced Security Guide Files

Many people want to be the competent people which can excel in the job in some area and be skillful in applying the knowledge to the practical working in some industry. But the thing is not so easy for them they need many efforts to achieve their goals. Passing the GH-500 test certification can make them become that kind of people and if you are one of them buying our GH-500 study materials will help you pass the GH-500 test smoothly with few efforts needed.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 2	• 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 3	• 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 4	• 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 5	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q49-Q54):

NEW QUESTION # 49

Which of the following Watch settings could you use to get Dependabot alert notifications? Each answer presents part of the solution. (Choose two.)

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

Answer: B,D

Explanation:
To receive Dependabot alert notifications for a repository, you can utilize the following Watch settings:
Custom setting: Allows you to tailor your notifications, enabling you to subscribe specifically to security alerts, including those from Dependabot.
All Activity setting: Subscribes you to all notifications for the repository, encompassing issues, pull requests, and security alerts like those from Dependabot.
The Participating and @mentions setting limits notifications to conversations you're directly involved in or mentioned, which may not include security alerts. The Ignore setting unsubscribes you from all notifications, including critical security alerts.

NEW QUESTION # 50
Which of the following is the most complete method for Dependabot to find vulnerabilities in third-party dependencies?

- A. The build tool finds the vulnerable dependencies and calls the Dependabot API
- B. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database
- C. Dependabot reviews manifest files in the repository
- D. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies

Answer: B

Explanation:
Dependabot builds a dependency graph by analyzing package manifests and lockfiles in your repository. This graph includes both direct and transitive dependencies. It then compares this graph against the GitHub Advisory Database, which includes curated, security-reviewed advisories.
This method provides a comprehensive and automated way to discover all known vulnerabilities across your dependency tree.

NEW QUESTION # 51
Which of the following options would close a Dependabot alert?

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

Answer: A

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 # 52
Using advanced setup, which code scanning configuration would help detect vulnerabilities before they are added to a shared branch?

- A. on:
  workflow_dispatch:
- B. on:

issues:

- C. on:
  pull_request:
- D. on:
  schedule:

Answer: C

Explanation:
Code scanning merge protection prevents a pull request from merging into a protected branch if it contains security issues or if required code scanning tools are missing or incomplete. This feature, configured using GitHub Rulesets>>, acts as a safeguard, blocking merges until all code scanning alerts are addressed to a defined severity level and the analysis is complete.
Code Scanning Configuration: You configure code scanning tools (like CodeQL) in your repository to run automatically on pull requests using the pull_request: event trigger.
Incorrect:
[Not A]
workflow_dispatch is a GitHub Actions trigger that allows users to manually start a workflow on demand, offering flexibility for tasks like deployments or testing that don't need to run automatically on every code change. This trigger can be configured with custom inputs to provide different parameters for each manual run, giving users more control over when and how specific workflows are executed.

NEW QUESTION # 53
Where can you use CodeQL analysis for code scanning? Each answer presents part of the solution. (Choose two.)

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

Answer: A,D

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 tabin pull requests only shows diff - not analysis results.

NEW QUESTION # 54
.....

www.pdfvce.com □ open and search for □ GH-500 □ to download for free □Test GH-500 Online

- Free PDF Unparalleled Microsoft - GH-500 - Latest GitHub Advanced Security Guide Files □ Search for ➽ GH-500 □ □ and download it for free immediately on 《 www.easy4engine.com 》 □GH-500 Reliable Test Cost
- 100% Pass Reliable Microsoft - Latest GH-500 Guide Files □ The page for free download of " GH-500 " on □ www.pdfvce.com □ will open immediately □GH-500 Test Certification Cost
- GitHub Advanced Security Exam Practice Dump Provide Best GH-500 Study Questions □ Search for ▹ GH-500 ◃ and easily obtain a free download on { www.practicevce.com } □Latest GH-500 Dumps Pdf
- Latest GH-500 Dumps Pdf □ Exam Topics GH-500 Pdf □ GH-500 Test Certification Cost □ Search on { www.pdfvce.com } for ✔ GH-500 □✔□ to obtain exam materials for free download □GH-500 Training Pdf
- GH-500 Valid Test Format □ GH-500 Exam Experience □ Test GH-500 Passing Score □ Download ➡ GH-500 □□□ for free by simply entering ☀ www.vceengine.com □☀□ website ☯GH-500 Reliable Exam Pdf
- The Importance of Microsoft GH-500 Exam Success for Future Microsoft Growth with Pdfvce □ Download □ GH-500 □ for free by simply searching on [www.pdfvce.com] □Test GH-500 Passing Score
- Exam Dumps GH-500 Collection □ Best GH-500 Preparation Materials □ Reliable GH-500 Exam Prep □ Search for [GH-500] on ▹ www.pass4test.com ◃ immediately to obtain a free download □GH-500 Training Pdf
- www.hongl.cc, daotao.wisebusiness.edu.vn, tutor1.gerta.pl, 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, 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, healoneself.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, iatdacademy.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, Disposable vapes

What's more, part of that Itcertkey GH-500 dumps now are free: https://drive.google.com/open?id=1Sl1_icGJFTm0TqBEEFE1wwSCaeEF-ScZ