Latest Test GH-500 Experience - GH-500 Test Answers

One failure makes many candidates fall into despair, become unconfident or even someone want to give up testing for IT certification. Now GH-500 reliable practice exam online will help you out. It covers most real test questions and will assist you to clear exam certainly. You will be confident in your test. GH-500 reliable practice exam online will be an important choice for your Microsoft certification. Sometimes choice is greater than effort.

Lead2PassExam promise that we will spare no effort to help you pass Microsoft certification GH-500 exam. Now you can free download part of practice questions and answers of Microsoft certification GH-500 exam on Lead2PassExam. When you select Lead2PassExam, you can not only pass Microsoft Certification GH-500 Exam, but also have one year free update service. Lead2PassExam can also promise if you fail to pass the exam, Lead2PassExam will 100% refund.

>> Latest Test GH-500 Experience <<

GH-500 Test Answers - Book GH-500 Free

Our study material is a high-quality product launched by the Lead2PassExam platform. And the purpose of our study material is to allow students to pass the professional qualification exams that they hope to see with the least amount of time and effort. If you are a child's mother, with GH-500 Test Answers, you will have more time to stay with your child; if you are a student, with GH-500 exam torrent, you will have more time to travel to comprehend the wonders of the world.

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	• 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 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 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.

Microsoft GitHub Advanced Security Sample Questions (Q74-Q79):

NEW QUESTION # 74

What happens when you enable secret scanning on a private repository?

- A. Repository administrators can view Dependabot alerts.
- B. Your team is subscribed to security alerts.
- C. Dependency review, secret scanning, and code scanning are enabled.
- D. GitHub performs a read-only analysis on the repository.

Answer: D

Explanation:
When secret scanning is enabled on a private repository, GitHub performs a read-only analysis of the repository's contents. This includes the entire Git history and files to identify strings that match known secret patterns or custom-defined patterns.
GitHub does not alter the repository, and enabling secret scanning does not automatically enable code scanning or dependency review - each must be configured separately.

NEW QUESTION # 75
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 manifest and lock files
- B. In the National Vulnerability Database
- C. In the dependency graph
- D. In security advisories reported on GitHub

Answer: B,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 # 76
What should you do after receiving an alert about a dependency added in a pull request?

- A. Disable Dependabot alerts for all repositories owned by your organization
- B. Update the vulnerable dependencies before the branch is merged
- C. Fork the branch and deploy the new fork
- D. Deploy the code to your default branch

Answer: B

Explanation:
If an alert is raised on a pull request dependency, best practice is to update the dependency to a secure version before merging the PR. This prevents the vulnerable version from entering the main codebase.
Merging or deploying the PR without fixing the issue exposes your production environment to known risks.

NEW QUESTION # 77
Which of the following secret scanning features can verify whether a secret is still active?

- A. Branch protection
- B. Validity checks
- C. Push protection

- D. Custom patterns

Answer: B

Explanation:
Validity checks, also called secret validation, allow GitHub to check if a detected secret is still active. If verified as live, the alert is marked as "valid", allowing security teams to prioritize the most critical leaks.
Push protection blocks secrets but does not check their validity. Custom patterns are user-defined and do not include live checks.

NEW QUESTION # 78
What is a prerequisite to define a custom pattern for a repository?

- A. Close other secret scanning alerts
- B. Specify additional match criteria
- C. Enable secret scanning
- D. Change the repository visibility to Internal

Answer: C

Explanation:
You must enable secret scanning before defining custom patterns. Secret scanning provides the foundational capability for detecting exposed credentials, and custom patterns build upon that by allowing organizations to specify their own regex-based patterns for secrets unique to their environment.
Without enabling secret scanning, GitHub will not process or apply custom patterns.

NEW QUESTION # 79
......

The last format is desktop GH-500 practice test software that can be accessed easily just by installing the software on the Windows Pc or Laptop. The desktop software format can be accessed offline without any internet so the students who don't have internet won't struggle in the preparation for GH-500 Exam. These three forms are specially made for the students to access them according to their comfort zone and GH-500 exam prepare for the best.

- lms24.blogdu.de, skillslibrary.in, www.stes.tyc.edu.tw, academy.kywdigital.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, app.csicosnet.com, Disposable vapes