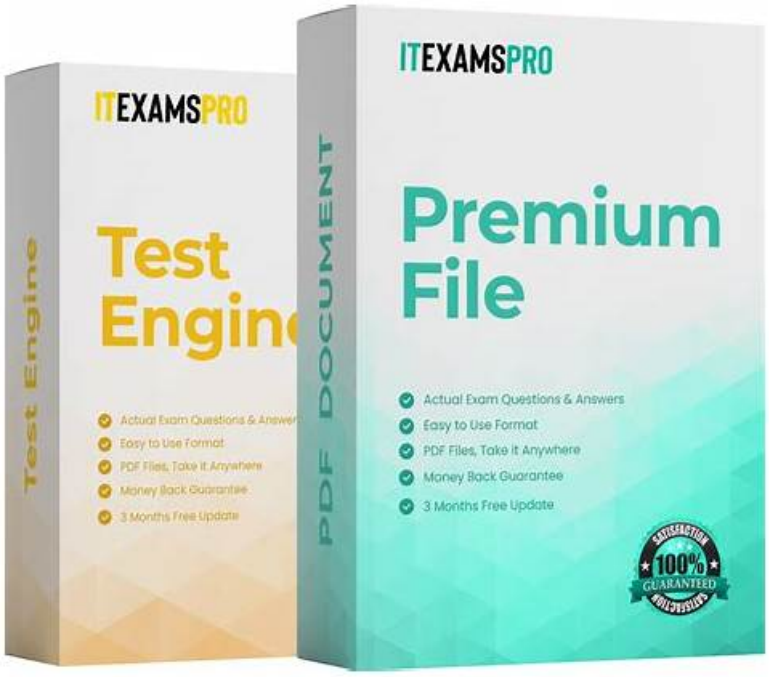
Reverse the Exam Anxiety By Getting the Real Microsoft GH-500 Dumps



What's more, part of that Free4Torrent GH-500 dumps now are free: https://drive.google.com/open?id=1NXlE35KVb_6WUtYcJ4ss5Q0ougGJK1DS

The Microsoft GH-500 exam questions in the web-based practice test are real and accurate. This GitHub Advanced Security (GH-500) practice exam is compatible with Mac, Linux, iOS, Android, and Windows. Likewise, no particular software installation or plugin is required because it is a browser-based GitHub Advanced Security (GH-500) practice exam. Chrome, Internet Explorer, Firefox, Safari, Opera, and all the major browsers support the web-based GitHub Advanced Security (GH-500) practice exam.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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.

Quiz 2026 Latest GH-500: Regualer GitHub Advanced Security Update

If you are determined to purchase our GitHub Advanced Security GH-500 valid exam collection materials for your companies, if you pursue long-term cooperation with site, we will have some relate policy. Firstly we provide one-year service warranty for every buyer who purchased Microsoft GH-500 valid exam collection materials.

Microsoft GitHub Advanced Security Sample Questions (Q40-Q45):

NEW QUESTION # 40
Which of the following statements most accurately describes push protection for secret scanning custom patterns?

- A. Push protection must be enabled for all, or none, of a repository's custom patterns.
- B. Push protection is an opt-in experience for each custom pattern.
- C. Push protection is not available for custom patterns.
- D. Push protection is enabled by default for new custom patterns.

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
Push protection for secret scanning custom patterns is an opt-in feature. This means that for each custom pattern defined in a repository, maintainers can choose to enable or disable push protection individually. This provides flexibility, allowing teams to enforce push protection on sensitive patterns while leaving it disabled for others.

NEW QUESTION # 41
How many alerts are created when two instances of the same secret value are in the same repository?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:
When multiple instances of the same secret value appear in a repository, only one alert is generated. Secret scanning works by identifying exposed credentials and token patterns, and it groups identical matches into a single alert to reduce noise and avoid duplication.
This makes triaging easier and helps teams focus on remediating the actual exposed credential rather than reviewing multiple redundant alerts.

NEW QUESTION # 42
What are Dependabot security updates?

- A. Compatibility scores to let you know whether updating a dependency could cause breaking changes to your project
- B. Automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities
- C. Automated pull requests to update the manifest to the latest version of the dependency
- D. Automated pull requests that help you update dependencies that have known vulnerabilities

Answer: D

Explanation:
Dependabot security updates are automated pull requests triggered when GitHub detects a vulnerability in a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to the minimum safe version that fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

NEW QUESTION # 43
What is a security policy?

- A. A security alert issued to a community in response to a vulnerability
- B. An alert about dependencies that are known to contain security vulnerabilities
- C. An automatic detection of security vulnerabilities and coding errors in new or modified code
- D. A file in a GitHub repository that provides instructions to users about how to report a security vulnerability

Answer: D

Explanation:
A security policy is defined by a SECURITY.md file in the root of your repository or .github/ directory. This file informs contributors and security researchers about how to responsibly report vulnerabilities. It improves your project's transparency and ensures timely

communication and mitigation of any reported issues.
Adding this file also enables a "Report a vulnerability" button in the repository's Security tab.

NEW QUESTION # 44
Which alerts do you see in the repository's Security tab? (Each answer presents part of the solution. Choose three.)

- A. Code scanning alerts
- B. Dependabot alerts
- C. Secret scanning alerts
- D. Repository permissions
- E. Security status alerts

Answer: A,B,C

Explanation:
In a repository's Security tab, you can view:
Secret scanning alerts: Exposed credentials or tokens
Dependabot alerts: Vulnerable dependencies from the advisory database
Code scanning alerts: Vulnerabilities in code detected via static analysis (e.g., CodeQL) You won't see general "security status alerts" (not a formal category) or permission-related alerts here.

NEW QUESTION # 45
.....

Our GH-500 exam torrent is highly regarded in the market of this field and come with high recommendation. Choosing our GH-500 exam guide will be a very promising start for you to begin your exam preparation because our GH-500 practice materials with high repute. Our GH-500 exam torrent is well reviewed in content made by the processional experts. They will instruct you on efficient points of knowledge to get familiar and remember high-effective. Besides, our GH-500 study tools galvanize exam candidates into taking actions efficiently. We are sure you will be splendid and get your desirable outcomes by our GH-500 exam guide. If your mind has made up then our GH-500 study tools will not let you down.

www.brightfuturetech.co.za, myportal.utt.edu.tt, Disposable vapes

What's more, part of that Free4Torrent GH-500 dumps now are free: https://drive.google.com/open?id=1NXlE35KVb_6WUtYcJ4ss5Q0ougGJK1DS