The best Microsoft certification GH-500 exam training mode released

12 best microsoft certifications for 2024
Microsoft Certified Azure Fundamentals
Microsoft Certified Data Analyst Associate
Microsoft Certified Azure Solutions Architect Expert
Microsoft Certified Windows Server Hybrid Administrator Associate
Microsoft Certified Associate
Microsoft Certified Azure AI Engineer Associate
Microsoft Certified Azure Data Engineer Associate
Microsoft Certified Azure Network Engineer Associate
Microsoft Certified Azure Security Engineer Associate
Microsoft Certified Dynamics 365 Fundamentals (CRM)
Microsoft Certified DevOps Engineer Expert
Microsoft Certified Expert
591Lab

What's more, part of that VCEEngine GH-500 dumps now are free: https://drive.google.com/open?id=1lvPiMPzvkBgrFTeWMpxW6Vwy6nbyg5y_

If you want to pass your exam and get your certification, we can make sure that our GH-500 guide questions will be your ideal choice. Our company will provide you with professional team, high quality service and reasonable price. In order to help customers solve problems, our company always insist on putting them first and providing valued service. We are living in the highly competitive world now. We have no choice but improve our soft power, such as get GH-500 Certification. It is of great significance to have GH-500 guide torrents to pass exams as well as highlight your resume, thus helping you achieve success in your workplace.

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	• 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 3	- 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 4	- 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 5	- 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.

VCEEngine Microsoft GH-500 Study Material In Different Forms

The thousands of Channel Partner Program GH-500 certification exam candidates have passed their dream GitHub Advanced Security GH-500 certification and they all used the valid and real Channel Partner Program GitHub Advanced Security GH-500 Exam Questions. You can also trust GitHub Advanced Security GH-500 pdf questions and practice tests.

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

NEW QUESTION # 49
What step is required to run a SARIF-compatible (Static Analysis Results Interchange Format) tool on GitHub Actions?

- A. Use the CLI to upload results to GitHub.
- B. The CodeQL action uploads the SARIF file automatically when it completes analysis.
- C. Update the workflow to include a final step that uploads the results.
- D. By default, the CodeQL runner automatically uploads results to GitHub on completion.

Answer: C

Explanation:
When using a SARIF-compatible tool within GitHub Actions, it's necessary to explicitly add a step in your workflow to upload the analysis results. This is typically done using the upload-sarif action, which takes the SARIF file generated by your tool and uploads it to GitHub for processing and display in the Security tab. Without this step, the results won't be available in GitHub's code scanning interface.

NEW QUESTION # 50
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

- A. workflow_dispatch
- B. commit
- C. trigger
- D. pull_request

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation:
Dependency review is triggered by specific events in GitHub workflows:
pull_request: When a pull request is opened, synchronized, or reopened, GitHub can analyze the changes in dependencies and provide a dependency review.
workflow_dispatch: This manual trigger allows users to initiate workflows, including those that perform dependency reviews.
The trigger and commit options are not recognized GitHub Actions events and would not initiate a dependency review.

NEW QUESTION # 51
Which details do you have to provide to create a custom pattern for secret scanning? (Each answer presents part of the solution. Choose two.)

- A. A list of repositories to scan
- B. Additional match requirements for the secret format
- C. The name of the pattern
- D. The secret format

Answer: C,D

Explanation:
When defining a custom pattern for secret scanning, two key fields are required:
Name of the pattern: A unique label to identify the pattern
Secret format: A regular expression that defines what the secret looks like (e.g., token format) You can optionally specify additional match requirements (like required context keywords), but they're not mandatory. Listing repositories is also not part of the required fields during pattern creation.

NEW QUESTION # 52
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 # 53
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. Dependabot reviews manifest files in the repository
- C. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies
- D. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database

Answer: D

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 # 54
......

GH-500 certification has great effect in this field and may affect your career even future. GH-500 real questions files are professional and has high passing rate so that users can pass exam at the first attempt. Many candidates compliment that GH-500 study guide materials are best assistant and useful for qualification exams, they have no need to purchase other training courses or books to study, and only by practicing ourGH-500 Exam Braindumps several times before exam, they can pass exam in short time easily. What are you waiting for?