GH-500 Prüfungen, GH-500 Prüfungs

Laden Sie die neuesten DeutschPrüfung GH-500 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1_q1-rCeahITKq6174ZM8w-KW4NNIVjRE

DeutschPrüfung ist eine Website, die alle Informationen zur verschiedenen Microsoft -Zertifizierungsprüfungen bieten kann. DeutschPrüfung kann die besten und neuesten Prüfungsressourcen für Sie bereitstellen. Wenn Sie DeutschPrüfung wählen, können Sie sich unbesorgt auf Ihre Microsoft GH-500 Zertifizierungsprüfung vorbereiten. Unsere Prüfungsunterlagen garantieren Ihnen, dass Sie 100% die Microsoft GH-500 Zertifizierungsprüfung bestehen können. Wenn nicht, geben wir Ihnen eine volle Rückerstattung oder akutualisieren schnell die Microsoft GH-500 Prüfungsfragen- und antworten. DeutschPrüfung kann Ihnen Hilfe bei der Microsoft GH-500 Zertifizierungsprüfung sowie bei Ihrer zukünftigen Arbeit bieten. Zwar gibt es viele Möglichkeiten, die Ihnen zu Ihrem Ziel verhelfen, aber es ist die klügste Wahl, wenn Sie DeutschPrüfung wählen. Mit DeutschPrüfung können Sie mit wenigem Geld die Prüfung sicherer bestehen. Außerdem bieten wir Ihnen einjährigen kostenlosen Update-Service.

Microsoft GH-500 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 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.

Thema 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.
Thema 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.
Thema 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.

GH-500 examkiller gültige Ausbildung Dumps & GH-500 Prüfung Überprüfung Torrents

Wenn Sie die Microsoft GH-500 Zertifizierungsprüfung bestehen wollen, ist es ganz notwendig, die Schulungsunterlagen von DeutschPrüfung zu wählen. Durch die Microsoft GH-500 Zertifizierungsprüfung wird Ihr Job besser garantiert. In Ihrem späten Berufsleben, werden Ihre Fertigkeiten und Kenntnisse wenigstens international akzeptiert. Das ist der Grund dafür, warum viele Menschen Microsoft GH-500 Zertifizierungsprüfung wählen. So ist diese Prüfung immer wichtiger geworden. Die Schulungsunterlagen zur Microsoft GH-500 Zertifizierungsprüfung von DeutschPrüfung, die von den erfahrungsreichen IT-Experten bearbeitet, wird Ihnen helfen, Ihren Wunsch zu erfüllen. Sie enthalten Prüfungsfragen und Antworten. Keine anderen Schulungsunterlagen sind DeutschPrüfung vergleichbar. Sie brauchen auch nicht am Kurs teilzunehmen. Sie brauchen nur die Schulungsunterlagen zur Microsoft GH-500 Zertifizierungsprüfung von DeutschPrüfung in den Warenkorb hinzufügen, dann können Sie mit Hilfe von DeutschPrüfung die Prüfung ganz einfach bestehen.

Microsoft GitHub Advanced Security GH-500 Prüfungsfragen mit Lösungen (Q28-Q33):

28. Frage
Which CodeQL query suite provides queries of lower severity than the default query suite?

- A. github/codeql/cpp/ql/src@main
- B. github/codeql-go/ql/src@main
- C. security-extended

Antwort: C

Begründung:
The security-extended query suite includes additional CodeQL queries that detect lower severity issues than those in the default security-and-quality suite.
About CodeQL query suites
With CodeQL code scanning, you can select a specific group of CodeQL queries, called a CodeQL query suite, to run against your code. The following built-in query suites are available through GitHub:
default query suite.
security-extended query suite. This suite is referred to as the "Extended" query suite on GitHub.
Currently, both the default query suite and the security-extended query suite are available for default setup for code scanning.

29. Frage
A dependency has a known vulnerability. What does the warning message include?

- A. How many projects use these components
- B. A brief description of the vulnerability
- C. An easily understandable visualization of dependency change
- D. The security impact of these changes

Antwort: B

Begründung:
When a vulnerability is detected, GitHub shows a warning that includes a brief description of the vulnerability. This typically covers the name of the CVE (if available), a short summary of the issue, severity level, and potential impact. The message also links to additional advisory data from the GitHub Advisory Database.
This helps developers understand the context and urgency of the vulnerability before applying the fix.

30. Frage
If default code security settings have not been changed at the repository, organization, or enterprise level, which repositories receive Dependabot alerts?

- A. repositories owned by an organization
- B. repositories owned by an enterprise account
- C. private repositories
- D. none

Antwort: D

Begründung:
When Dependabot detects vulnerable dependencies in your repositories, we generate a Dependabot alert and display it on the Security tab for the repository. GitHub notifies the maintainers of affected repositories about the new alert according to their notification preferences.
Dependabot is enabled by default on all public repositories, and needs to be enabled on private repositories.
Note:
By default, no repositories receive Dependabot alerts unless configuration is explicitly enabled.
GitHub does not enable Dependabot alerts automatically for any repositories unless:
The feature is turned on manually
It's configured at the organization or enterprise level via security policies This includes public, private, and enterprise-owned repositories -manual activation is required.

31. Frage
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 an external continuous integration (CI) system
- D. In a third-party Git repository

Antwort: A,C

Begründung:
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 tab in pull requests only shows diff - not analysis results.

32. Frage
A colleague ignores a code scanning alert. What are the implications of the colleague's action?
Each answer presents part of the solution. (Choose three.)

- A. Data could be used insecurely.
- B. A dangerous argument could be passed to functions.
- C. Webhooks and the code scanning API remove the alert.
- D. GitHub removes the alert after sixty days.
- E. Sensitive information could be leaked.

Antwort: A,B,E

Begründung:
If you configure code scanning using CodeQL, you can also find data-flow problems in your code.
Data-flow analysis finds potential security issues in code, such as: using data insecurely[C], passing dangerous arguments to functions [D], and leaking sensitive information[B].
When code scanning reports data-flow alerts, GitHub shows you how data moves through the code. Code scanning allows you to identify the areas of your code that leak sensitive information, and that could be the entry point for attacks by malicious users.

33. Frage
.....

- GH-500 Prüfungsunterlagen □ GH-500 Deutsche □ GH-500 Prüfungsunterlagen □ Öffnen Sie 「 www.it-pruefung.com 」 geben Sie 「 GH-500 」 ein und erhalten Sie den kostenlosen Download □GH-500 Online Prüfung
- GH-500 Fragen&Antworten □ GH-500 Prüfungs-Guide □ GH-500 Fragen&Antworten □ Suchen Sie jetzt auf ➤ www.itzert.com □ nach □ GH-500 □ und laden Sie es kostenlos herunter □GH-500 Prüfungen
- GH-500 Testengine □ GH-500 Deutsch Prüfungsfragen □ GH-500 Prüfungen □ Suchen Sie auf der Webseite ➽ www.echtefrage.top □ nach 【 GH-500 】 und laden Sie es kostenlos herunter □GH-500 Prüfungsunterlagen
- academy.quantalgos.in, blogfreely.net, www.dkcomposite.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, myportal.utt.edu.tt, www.zsflt.top, myportal.utt.edu.tt, www.stes.tyc.edu.tw, dkpacademy.in, 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, Disposable vapes

Außerdem sind jetzt einige Teile dieser DeutschPrüfung GH-500 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1_q1-rCeahlTKq6174ZM8w-KW4NNIVjRE