熱門的GitHub-Advanced-Security PDF題庫|高通過率的考試材料|受信任的GitHub-Advanced-Security：GitHub Advanced Security GHAS Exam

從Google Drive中免費下載最新的KaoGuTi GitHub-Advanced-Security PDF版考試題庫：https://drive.google.com/open?id=1cZcGIwmG8tsr3g3ZtyUa15pj_IrZmXjh

大家在準備考試的時候，可以結合本網站最新的 GitHub GitHub-Advanced-Security 擬真試題去認真地做練習，這樣的話，可以為你的考試節省很多的時間。GitHub 的 GitHub-Advanced-Security 考試整體來說還是不算複雜的，只要事先將擬真試題看好就沒有問題了。還有，做實驗題是要一定要多想想，這樣的話，才能將自身的一些素質提高上去。我們的考題網剛更新 GitHub-Advanced-Security 題庫能確保考生能順利通過 GitHub-Advanced-Security 考試，獲得 GitHub 認證證照。

GitHub GitHub-Advanced-Security 考試大綱：

主題	簡介
主題 1	• Describe GitHub Advanced Security best practices: This section of the exam measures skills of a GitHub Administrator and covers outlining recommended strategies for adopting GitHub Advanced Security at scale. Test?takers will explain how to apply security policies, enforce branch protections, shift left security checks, and use metrics from GHAS tools to continuously improve an organization’s security posture.
主題 2	• Configure and use code scanning: This section of the exam measures skills of a DevSecOps Engineer and covers enabling and customizing GitHub code scanning with built?in or marketplace rulesets. Examinees must know how to interpret scan results, triage findings, and configure exclusion or override settings to reduce noise and focus on high?priority vulnerabilities.

主題 3	• Configure and use dependency management: This section of the exam measures skills of a DevSecOps Engineer and covers configuring dependency management workflows to identify and remediate vulnerable or outdated packages. Candidates will show how to enable Dependabot for version updates, review dependency alerts, and integrate these tools into automated CI • CD pipelines to maintain secure software supply chains.
主題 4	• Describe the GHAS security features and functionality: This section of the exam measures skills of a GitHub Administrator and covers identifying and explaining the built?in security capabilities that GitHub Advanced Security provides. Candidates should be able to articulate how features such as code scanning, secret scanning, and dependency management integrate into GitHub repositories and workflows to enhance overall code safety.
主題 5	• Configure GitHub Advanced Security tools in GitHub Enterprise: This section of the exam measures skills of a GitHub Administrator and covers integrating GHAS features into GitHub Enterprise Server or Cloud environments. Examinees must know how to enable advanced security at the enterprise level, manage licensing, and ensure that scanning and alerting services operate correctly across multiple repositories and organizational units.
主題 6	• Configure and use secret scanning: This section of the exam measures skills of a DevSecOps Engineer and covers setting up and managing secret scanning in organizations and repositories. Test?takers must demonstrate how to enable secret scanning, interpret the alerts generated when sensitive data is exposed, and implement policies to prevent and remediate credential leaks.

GitHub-Advanced-Security考試資訊，新版GitHub-Advanced-Security考古題

KaoGuTi的IT專家團隊利用他們的經驗和知識不斷的提升考試培訓材料的品質，來滿足每位考生的需求，保證考生第一次參加GitHub GitHub-Advanced-Security認證考試順利的通過，你們通過購買KaoGuTi的產品總是能夠更快得到更新更準確的考試相關資訊，KaoGuTi的產品的覆蓋面很大很廣，可以為很多參加IT認證考試的考生提供方便，而且準確率100%，能讓你安心的去參加考試，並通過獲得認證。

最新的 GitHub Certification GitHub-Advanced-Security 免費考試真題 (Q55-Q60):

問題 #55
What are Dependabot security updates?

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

答案：A

解題說明：
Dependabot security updatesareautomated pull requeststriggered when GitHub detects avulnerabilityin a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to theminimum safe versionthat fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

問題 #56
Which Dependabot configuration fields are required? (Each answer presents part of the solution. Choose three.)

- A. package-ecosystem

- B. milestone
- C. schedule.interval
- D. allow
- E. directory

答案： A,C,E

解題說明：
Comprehensive and Detailed Explanation:
When configuring Dependabot via the dependabot.yml file, the following fields are mandatory for each update configuration:
directory: Specifies the location of the package manifest within the repository. This tellsDependabot where to look for dependency files.
package-ecosystem: Indicates the type of package manager (e.g., npm, pip, maven) used in the specified directory.
schedule.interval: Defines how frequently Dependabot checks for updates (e.g., daily, weekly). This ensures regular scanning for outdated or vulnerable dependencies.
The milestone field is optional and used for associating pull requests with milestones. The allow field is also optional and used to specify which dependencies to update.
GitLab

問題 #57
Assuming there is no custom Dependabot behavior configured, where possible, what does Dependabot do after sending an alert about a vulnerable dependency in a repository?

- A. Scans any push to all branches and generates an alert for each vulnerable repository
- B. Scans repositories for vulnerable dependencies on a schedule and adds those files to a manifest
- C. Creates a pull request to upgrade the vulnerable dependency to the minimum possible secure version
- D. Constructs a graph of all the repository's dependencies and public dependents for the default branch

答案： C

解題說明：
After generating an alert for a vulnerable dependency, Dependabot automatically attempts to create a pull request to upgrade that dependency to theminimum required secure version-if a fix is available and compatible with your project.
This automated PR helps teams fix vulnerabilities quickly with minimal manual intervention. You can also configure update behaviors using dependabot.yml, but in the default state, PR creation is automatic.

問題 #58
Secret scanning will scan:

- A. A continuous integration system.
- B. External services.
- C. Any Git repository.
- D. The GitHub repository.

答案： D

解題說明：
Secret scanning is a feature provided by GitHub that scans the contents of your GitHub repositories for known types of secrets, such as API keys and tokens. It operates within the GitHub environment and does not scan external systems, services, or repositories outside of GitHub. Its primary function is to prevent the accidental exposure of sensitive information within your GitHub-hosted code.

問題 #59
Which of the following features helps to prioritize secret scanning alerts that present an immediate risk?

- A. Push protection
- B. Custom pattern dry runs
- C. Non-provider patterns

- D. Secret validation

答案：D

解題說明：
Secret validationchecks whether a secret found in your repository is still valid and active with the issuing provider (e.g., AWS, GitHub, Stripe). If a secret is confirmed to be active, the alert ismarked as verified, which means it's considered ahigh-priority issuebecause it presents an immediate security risk.
This helps teams respond faster tovalid, exploitablesecrets rather than wasting time on expired or fake tokens.

問題 #60
.....

順便提一下，可以從雲存儲中下載KaoGuTi GitHub-Advanced-Security考試題庫的完整版：https://drive.google.com/open?id=1cZcGIwmG8tsr3g3ZtyUa15pj_IrZmXjh