퍼펙트한GH-500시험패스자료덤프데모문제다운받기

2026 PassTIP 최신 GH-500 PDF 버전 시험 문제집과 GH-500 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1SHtQ88K0wQA3D3A7q5kKRb4_ryTMu-Da

여러분은 우선 우리 PassTIP사이트에서 제공하는Microsoft인증GH-500시험덤프의 일부 문제와 답을 체험해보세요. 우리 PassTIP를 선택해주신다면 우리는 최선을 다하여 여러분이 꼭 한번에 시험을 패스할 수 있도록 도와드리겠습니다.만약 여러분이 우리의 인증시험덤프를 보시고 시험이랑 틀려서 패스를 하지 못하였다면 우리는 무조건 덤프 비용전부를 환불해드립니다.

Microsoft GH-500 시험요강:

주제	소개

주제 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.
주제 2	• 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.
주제 3	• 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.
주제 4	• 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.
주제 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-500최신버전 덤프샘플문제 - GH-500시험패스 가능 덤프

지금 같은 정보시대에, 많은 IT업체 등 사이트에Microsoft GH-500인증관련 자료들이 제공되고 있습니다, 하지만 이런 사이트들도 정확하고 최신 시험자료 확보는 아주 어렵습니다. 그들의Microsoft GH-500자료들은 아주 기본적인 것들뿐입니다. 전면적이지 못하여 응시자들의 관심을 쌓지 못합니다.

최신 GitHub Administrator GH-500 무료샘플문제 (Q56-Q61):

질문 # 56
Which of the following secret scanning features can verify whether a secret is still active?

- A. Push protection
- B. Branch protection
- C. Validity checks
- D. Custom patterns

정답：C

설명：
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.

질문 # 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. Constructs a graph of all the repository's dependencies and public dependents for the default branch
- C. Scans repositories for vulnerable dependencies on a schedule and adds those files to a manifest
- D. Creates a pull request to upgrade the vulnerable dependency to the minimum possible secure version

정답：D

설명：
After generating an alert for a vulnerable dependency, Dependabot automatically attempts to create a pull request to upgrade that dependency to the minimum 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.

질문 # 58
Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

- A. A repository member of an enterprise organization
- B. A user who has write access to the repository
- C. A user who has read access to the repository
- D. An enterprise administrator

정답：B

설명：
Comprehensive and Detailed Explanation:
By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.
Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.

질문 # 59
What is the first step you should take to fix an alert in secret scanning?

- A. Revoke the alert if the secret is still valid.
- B. Remove the secret in a commit to the main branch.
- C. Archive the repository.
- D. Update your dependencies.

정답：A

설명：
The first step when you receive a secret scanning alert is to revoke the secret if it is still valid. This ensures the secret can no longer be used maliciously. Only after revoking it should you proceed to remove it from the code history and apply other mitigation steps. Simply deleting the secret from the code does not remove the risk if it hasn't been revoked - especially since it may already be exposed in commit history.

질문 # 60
Which of the following options are code scanning application programming interface (API) endpoints? (Each answer presents part of the solution. Choose two.)

- A. Modify the severity of an open code scanning alert
- B. Delete all open code scanning alerts
- C. List all open code scanning alerts for the default branch
- D. Get a single code scanning alert

정답：C,D

설명：
The GitHub Code Scanning API includes endpoints that allow you to:
List alerts for a repository (filtered by branch, state, or tool) - useful for monitoring security over time.
Get a single alert by its ID to inspect its metadata, status, and locations in the code.
However, GitHub does not support modifying the severity of alerts via API - severity is defined by the scanning tool (e.g., CodeQL). Likewise, alerts cannot be deleted via the API; they are resolved by fixing the code or dismissing them manually.

질문 # 61
.....

- 최신버전 GH-500시험패스자료 완벽한 시험 최신버전 덤프 □ 《 www.itdumpskr.com 》을(를) 열고□ GH-500 □를 검색하여 시험 자료를 무료로 다운로드하십시오GH-500시험대비 최신 덤프모음집
- GH-500합격보장 가능 덤프공부 □ GH-500합격보장 가능 덤프공부 □ GH-500최고덤프샘플 □ 시험 자료를 무료로 다운로드하려면▷ www.dumptop.com◁을 통해□ GH-500 □를 검색하십시오GH-500최고덤프샘플
- GH-500시험대비 덤프문제 □ GH-500시험패스 인증공부자료 □ GH-500덤프최신버전 □ ☀ www.itdumpskr.com □☀□웹사이트에서□ GH-500 □를 열고 검색하여 무료 다운로드GH-500인증덤프공부
- 높은 통과율 GH-500시험패스자료 덤프로 시험패스는 한방에 가능 □ ➽ www.pass4test.net □웹사이트를 열고✔ GH-500 □✔□를 검색하여 무료 다운로드GH-500최고덤프샘플
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, edu.canadahebdo.ca, 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.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

그리고 PassTIP GH-500 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1SHtQ88K0wQA3D3A7q5kKRb4_ryTMu-Da