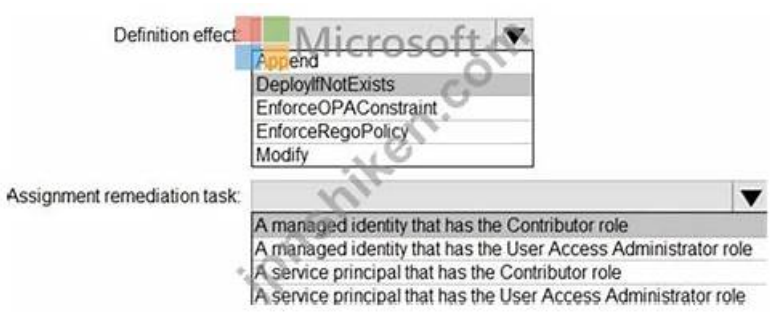
素敵なGH-500問題トレーリング |最初の試行で簡単に勉強して試験に合格する &最高のMicrosoft GitHub Advanced Security



ちなみに、Jpexam GH-500の一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1wsdtTnPkryKLLDxeKyNRKIWLrH2RnME3

JpexamのGH-500問題集を使用した後、あなたはたくさんののGH-500試験資料を勉強するとか、専門のトレーニング機構に参加するとかなど必要がないと認識します。Jpexam GH-500問題集は試験の範囲を広くカバーするだけでなく、質は高いです。JpexamのGH-500問題集を購入し勉強するだけ、あなたは試験にたやすく合格できます。

我々Jpexamから一番質高いGH-500問題集を見つけられます。弊社のMicrosoftのGH-500練習問題の通過率は他のサイトに比較して高いです。あなたは我が社のGH-500練習問題を勉強して、試験に合格する可能性は大きくなります。MicrosoftのGH-500資格認定証明書を取得したいなら、我々の問題集を入手してください。

>> GH-500問題トレーリング <<

GH-500合格資料 & GH-500合格率

有効なGH-500研究急流がなければ、あなたの利益はあなたの努力に比例しないといつも感じていますか？ あなたは常に先延ばしに苦しみ、散発的な時間を十分に活用できないと感じていますか？ 答えが完全に「はい」の場合は、GH-500の高品質で効率的なテストツールであるGH-500トレーニング資料を試してみることをお勧めします。 GH-500試験に合格し、夢のある認定資格を取得することで、あなたの成功は100％保証され、より高い収入やより良い企業へのより多くの機会を得ることができます。

Microsoft GH-500 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• CodeQL を使用したコードスキャンの設定と使用: このドメインでは、CodeQL とサードパーティツールの両方を使用したコードスキャンにおけるアプリケーションセキュリティアナリストと DevSecOps エンジニアのスキルを測定します。コードスキャンの有効化、開発ライフサイクルにおけるコードスキャンの役割、CodeQL の有効化とサードパーティ分析の違い、GitHub Actions ワークフローと他の CI ツールでの CodeQL の実装、SARIF 結果のアップロード、ワークフロー頻度の設定とイベントのトリガー、アクティブリポジトリのワークフローテンプレートの編集、CodeQL スキャン結果の表示、ワークフローの失敗のトラブルシューティングと設定のカスタマイズ、コード全体のデータフローの分析、リンクされたドキュメントによるコードスキャンアラートの解釈、アラートを閉じるタイミングの決定、コンパイルと言語サポートに関連する CodeQL の制限の理解、SARIF カテゴリの定義などをカバーします。

トピック 2	• GitHub Advanced Security のベスト プラクティス、結果、および是正措置の実施方法を説明する: このセクションでは、セキュリティ マネージャーと開発チーム リーダーが GHAS の結果を効果的に処理し、ベスト プラクティスを適用するスキルを評価します。これには、共通脆弱性識別子 (CVE) と共通弱点列挙 (CWE) の識別子を使用してアラートを説明し、修復を提案すること、ドキュメントとデータに基づく決定を含むアラートをクローズまたは却下するための意思決定プロセス、デフォルトの CodeQL クエリ スイートの理解、CodeQL がコンパイル言語とインタープリタ言語を分析する方法、ワークフローにおける開発チームとセキュリティ チームの役割と責任、コード スキャンのプル リクエスト ステータス チェックの重大度しきい値の調整、フィルターを使用したシークレット スキャンの修復の優先順位付け、リポジトリ ルールセットによる CodeQL と依存関係レビューのワークフローの適用、プル リクエスト中やプッシュ保護の有効化など、開発ライフサイクルの早い段階で脆弱性を検出して修復するためのコード スキャン、シークレット スキャン、依存関係分析の構成が含まれます。
トピック 3	• シークレットスキャンの設定と使用：このドメインは、シークレットスキャンの設定と管理スキルを持つDevOpsエンジニアとセキュリティアナリストを対象としています。シークレットスキャンとは何か、そしてシークレットの漏洩を防ぐプッシュ保護機能について理解することが含まれます。受験者は、パブリックリポジトリとプライベートリポジトリでのシークレットスキャンの可用性の違いを理解し、プライベートリポジトリでのスキャンを有効にし、アラートに適切に対応する方法を習得します。このドメインでは、シークレットのアラート生成基準、ユーザーロールベースのアラート表示と通知、デフォルトのスキャン動作のカスタマイズ、管理者以外のアラート受信者の割り当て、スキャンからのファイルの除外、リポジトリ内でのカスタムシークレットスキャンの有効化について学習します。
トピック 4	• Dependabot と Dependency Review の設定と使用: ソフトウェア エンジニアと脆弱性管理スペシャリストを対象としたこのセクションでは、依存関係の脆弱性を管理するためのツールについて説明します。受験者は、依存関係グラフとその生成方法、ソフトウェア部品表 (SBOM) の概念と形式、依存関係の脆弱性の定義、Dependabot のアラートとセキュリティ更新、および Dependency Review 機能について学習します。依存関係グラフと GitHub Advisory Database に基づいてアラートが生成される方法、Dependabot と Dependency Review の違い、プライベート リポジトリと組織でのこれらのツールの有効化と設定、デフォルトのアラート設定、必要な権限、Dependabot 設定ファイルの作成とアラートの自動消去ルール、ライセンス チェックや重大度しきい値などの Dependency Review ワークフローの設定、通知の設定、アラートやプル リクエストからの脆弱性の特定、セキュリティ更新の有効化、プル リクエストのテストやマージなどの修復アクションの実行についても説明します。
トピック 5	• GHAS のセキュリティ機能について説明する: 試験のこのセクションでは、セキュリティ エンジニアとソフトウェア開発者のスキルを測定し、全体的なセキュリティ エコシステムにおける GitHub Advanced Security (GHAS) 機能の役割を理解することが対象となります。受験者は、オープンソース プロジェクトで自動的に利用できるセキュリティ機能と、GHAS を GitHub Enterprise Cloud (GHEC) または GitHub Enterprise Server (GHES) と組み合わせることでロック解除されるセキュリティ機能を区別する方法を学習します。このドメインには、セキュリティ概要ダッシュボード、シークレット スキャンとコード スキャンの違い、シークレット スキャン、コード スキャン、Dependabot が連携してソフトウェア開発ライフサイクルを保護する仕組みに関する知識が含まれます。また、開発ライフサイクル全体にわたる独立したセキュリティ レビューと統合セキュリティを比較するシナリオ、マニフェストと脆弱性データベースを使用して脆弱な依存関係を検出する方法、アラートへの適切な対応、アラートを無視するリスク、アラートに対する開発者の責任、アラートを表示するためのアクセス管理、開発プロセスにおける Dependabot アラートの配置についても取り上げます。

Microsoft GitHub Advanced Security 認定 GH-500 試験問題 (Q72-Q77):

質問 # 72
You have enabled security updates for a repository. When does GitHub mark a Dependabot alert as resolved for that repository?

- A. When you merge a pull request that contains a security update
- B. When Dependabot creates a pull request to update dependencies
- C. When the pull request checks are successful
- D. When you dismiss the Dependabot alert

正解：A

解説：
A Dependabot alert is marked as resolved only after the related pull request is merged into the repository. This indicates that the vulnerable dependency has been officially replaced with a secure version in the active codebase.
Simply generating a PR or passing checks does not change the alert status; merging is the key step.

質問 # 73
What is a security policy?

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

正解：A

解説：
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.

質問 # 74
When secret scanning detects a set of credentials on a public repository, what does GitHub do?

- A. It displays a public alert in the Security tab of the repository.
- B. It sends a notification to repository members.
- C. It notifies the service provider who issued the secret.
- D. It scans the contents of the commits for additional secrets.

正解：C

解説：
When a public repository contains credentials that match known secret formats, GitHub will automatically notify the service provider that issued the secret. This process is known as "secret scanning partner notification". The provider may then revoke the secret or contact the user directly.
GitHub does not publicly display the alert and does not send internal repository notifications for public detections.

質問 # 75
Which of the following Watch settings could you use to get Dependabot alert notifications? (Each answer presents part of the solution. Choose two.)

- A. The All Activity setting
- B. The Ignore setting
- C. The Custom setting
- D. The Participating and @mentions setting

正解：A、C

解説：
Comprehensive and Detailed Explanation:
To receive Dependabot alert notifications for a repository, you can utilize the following Watch settings:

Custom setting: Allows you to tailor your notifications, enabling you to subscribe specifically to security alerts, including those from Dependabot.
All Activity setting: Subscribes you to all notifications for the repository, encompassing issues, pull requests, and security alerts like those from Dependabot.
The Participating and @mentions setting limits notifications to conversations you're directly involved in or mentioned, which may not include security alerts. The Ignore setting unsubscribes you from all notifications, including critical security alerts.
GitHub Docs
+1
GitHub Docs
+1

質問 # 76
How do I configure a webhook to monitor key scan alert events? What are the steps of this operation?

- A. Configure a webhook to monitor for secret scanning alert events.
- B. Document alternatives to storing secrets in the source code.
- C. Dismiss alerts that are older than 90 days.
- D. Enable system for cross-domain identity management (SCIM) provisioning for the enterprise.

正解：A、B

解説：
To proactively address secret scanning:
Webhooks can be configured to listen for secret scanning events. This allows automation, logging, or alerting in real-time when secrets are detected.
Documenting secure development practices (like using environment variables or secret managers) helps reduce the likelihood of developers committing secrets in the first place.
Dismissal based on age is not a best practice without triage. SCIM deals with user provisioning, not scanning alerts.

質問 # 77
.....

www.goshiken.com □を開き、【 GH-500 】を検索して無料でダウンロードしてくださいGH-500トレーニング費用

- GH-500日本語的中対策 □ GH-500勉強の資料 □ GH-500入門知識 □ ✔ www.goshiken.com □✔□で《 GH-500 》を検索して、無料でダウンロードしてくださいGH-500受験準備
- www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mahiracademy.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

さらに、Jpexam GH-500ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1wsdtTnPkryKLLDxeKyNRKIWLrH2RnME3