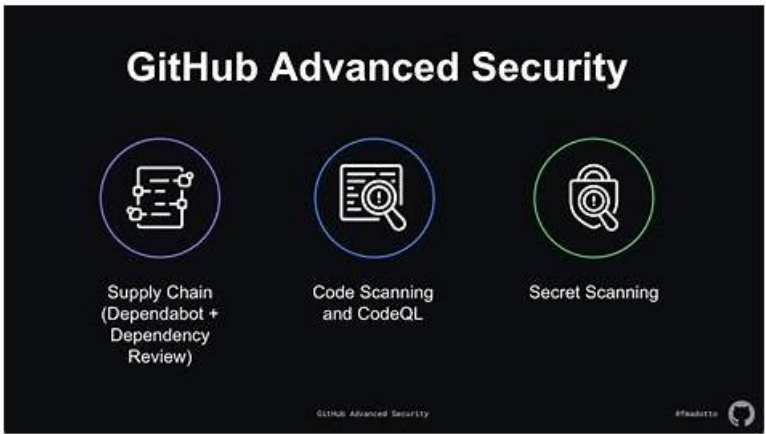


GitHub-Advanced-Security的中率 & GitHub-Advanced-Security技術試験



BONUS!!! Japancert GitHub-Advanced-Securityダンプの一部を無料でダウンロード: <https://drive.google.com/open?id=1QMA2Ln5VN4NNflcZ21umolusXD1YgGVg>

GitHubのGitHub-Advanced-Security試験は国際的に認可されます。これがあったら、よい高い職位の通行証を持っているようです。Japancertの提供するGitHubのGitHub-Advanced-Security試験の資料とソフトは経験が豊富なITエリートに開発されて、何回も更新されています。何十ユーロだけでこのような頼もしいGitHubのGitHub-Advanced-Security試験の資料を得ることができます。試験に合格してからあなたがよりよい仕事と給料がもらえるかもしれません。

このほど、今のIT会社は多くのIT技術人材を急速に需要して、あなたはこのラッキーな人になりたいですか? GitHubのGitHub-Advanced-Security試験に参加するのはあなたに自身のレベルを高めさせるだけでなく、あなたがより良く就職し輝かしい未来を持っています。弊社JapancertはGitHubのGitHub-Advanced-Security問題集を購入し勉強した後、あなたはGitHub-Advanced-Security試験に合格することでできると信じています。

>> GitHub-Advanced-Security的中率 <<

試験の準備方法-素敵な GitHub-Advanced-Security的中率試験-実際的な GitHub-Advanced-Security技術試験

GitHub-Advanced-Security認証試験に合格したいのは簡単ではなく、いい復習方法は必要です。我々はあなたに詳しい問題と答えがあるGitHub-Advanced-Security問題集を提供します。この問題集は我々の経験がある専門家たちによって開発されています。我々のすばらしいGitHub-Advanced-Security問題集はお客様の試験への成功を確保することができます。

GitHub GitHub-Advanced-Security 認定試験の出題範囲:

トピック	出題範囲
トピック 1	シークレットスキャンの設定と使用: この試験セクションでは、DevSecOpsエンジニアのスキルを評価し、組織およびリポジトリにおけるシークレットスキャンの設定と管理について学習します。受験者は、シークレットスキャンを有効にする方法、機密データが漏洩した際に生成されるアラートを解釈する方法、そして認証情報の漏洩を防止および修復するためのポリシーを実装する方法を実証する必要があります。

トピック 2	GitHub EnterpriseでGitHub Advanced Securityツールを構成する：この試験セクションでは、GitHub管理者のスキルを評価し、GHAS機能をGitHub Enterprise ServerまたはCloud環境に統合する方法を網羅します。受験者は、エンタープライズレベルで高度なセキュリティを有効化する方法、ライセンスを管理する方法、そして複数のリポジトリと組織単位にわたってスキャンおよびアラートサービスが正しく動作することを保証する方法を理解する必要があります。
トピック 3	CodeQLを使用したコードスキャン：この試験セクションでは、DevSecOpsエンジニアのスキルを評価し、より深いセマンティック分析のためのクエリの作成またはカスタマイズをCodeQLを用いて行います。受験者は、CodeQLワークフローの設定方法、クエリスイートの理解方法、そしてCodeQLアラートの解釈方法を実証し、標準的な静的分析では発見できない複雑なコードの問題を発見する必要があります。
トピック 4	GitHub Advanced Securityのベストプラクティスを説明する：このセクションでは、GitHub管理者のスキルを評価し、GitHub Advanced Securityを大規模に導入するための推奨戦略の概要を説明します。受験者は、セキュリティポリシーの適用方法、ブランチ保護の強化方法、セキュリティチェックのシフトレフト方法、そしてGHASツールのメトリクスを活用して組織のセキュリティ体制を継続的に改善する方法を説明できるようになります。
トピック 5	- 依存関係管理の設定と使用：この試験セクションでは、DevSecOpsエンジニアのスキルを評価し、脆弱性のあるパッケージや古いパッケージを特定して修正するための依存関係管理ワークフローの設定について学習します。受験者は、Dependabotを使用してバージョン更新を有効化する方法、依存関係アラートを確認する方法、そしてこれらのツールを自動化されたCI - CDパイプラインに統合して安全なソフトウェアサプライチェーンを維持する方法を示すことができます。
トピック 6	コードスキャンの設定と使用：この試験セクションでは、DevSecOpsエンジニアのスキルを評価し、組み込みルールセットまたはマーケットプレイスルールセットを使用してGitHubコードスキャンを有効化およびカスタマイズする方法を扱います。受験者は、スキャン結果の解釈方法、検出結果のトリアージ方法、そしてノイズを減らして優先度の高い脆弱性に焦点を当てるための除外設定またはオーバーライド設定を行う方法を理解する必要があります。

GitHub Advanced Security GHAS Exam 認定 GitHub-Advanced-Security 試験問題 (Q73-Q78):

質問 # 73

Which alerts do you see in the repository's Security tab? (Each answer presents part of the solution. Choose three.)

- A. Repository permissions
- B. Security status alerts
- C. Secret scanning alerts
- D. Code scanning alerts
- E. Dependabot alerts

正解: C、D、E

解説:

In a repository's Security tab, you can view:

* Secret scanning alerts: Exposed credentials or tokens

* Dependabot alerts: Vulnerable dependencies from the advisory database

* Code scanning alerts: Vulnerabilities in code detected via static analysis (e.g., CodeQL) You won't see general "security status alerts" (not a formal category) or permission-related alerts here.

質問 # 74

Which key is required in the update settings of the Dependabot configuration file?

- A. commit-message
- B. rebase-strategy
- C. package-ecosystem
- D. assignees

正解: C

解説:

In a dependabot.yml configuration file, package-ecosystem is a required key. It defines the package manager being used in that update configuration (e.g., npm, pip, maven, etc.).

Without this key, Dependabot cannot determine how to analyze or update dependencies. Other keys like rebase-strategy or commit-message are optional and used for customizing behavior.

質問 # 75

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

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

正解: B

解説:

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.

質問 # 76

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

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

正解: A

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 # 77

You are a maintainer of a repository and Dependabot notifies you of a vulnerability. Where could the vulnerability have been disclosed? (Each answer presents part of the solution. Choose two.)

- A. In the dependency graph
- B. In manifest and lock files
- C. In the National Vulnerability Database
- D. In security advisories reported on GitHub

正解: C、D

解説:

Comprehensive and Detailed Explanation:

Dependabot alerts are generated based on data from various sources:

National Vulnerability Database (NVD): A comprehensive repository of known vulnerabilities, which GitHub integrates into its advisory database.

GitHub Docs

Security Advisories Reported on GitHub: GitHub allows maintainers and security researchers to report and discuss vulnerabilities, which are then included in the advisory database.

The dependency graph and manifest/lock files are tools used by GitHub to determine which dependencies are present in a repository but are not sources of vulnerability disclosures themselves.

質問 # 78

.....

クライアントがGitHub-Advanced-Security学習実践ガイドを購入する前に、無料の試用版を無料で入手できます。クライアントは、当社のウェブサイトログインして、製品のページにアクセスできます。製品のページには、GitHub-Advanced-Security試験資料に関する多くの重要な情報がリストされており、製品の価格、バージョン、更新時間、試験名とコード、質問と回答の合計額、GitHub-Advanced-Security便利なテストガイドと割引。この情報を見た後、GitHub-Advanced-Security有用なテストガイドを包括的に理解できます。

GitHub-Advanced-Security技術試験: <https://www.japancert.com/GitHub-Advanced-Security.html>

- GitHub-Advanced-Security関連日本語内容 □ GitHub-Advanced-Security日本語版テキスト内容 □ GitHub-Advanced-Security受験対策書 □ “www.passtest.jp”から簡単に⇒ GitHub-Advanced-Security⇐を無料でダウンロードできますGitHub-Advanced-Security過去問題
- 試験の準備方法-検証するGitHub-Advanced-Security的中率試験-素晴らしいGitHub-Advanced-Security技術試験 ⇔ 今すぐ{ www.goshiken.com }を開き、⇒ GitHub-Advanced-Security⇐を検索して無料でダウンロードしてくださいGitHub-Advanced-Securityテスト対策書
- 試験の準備方法-有効的なGitHub-Advanced-Security的中率試験-ハイパスレートのGitHub-Advanced-Security技術試験 □ ➡ GitHub-Advanced-Security □を無料でダウンロード ➡ www.passtest.jp □ ウェブサイトを入力するだけGitHub-Advanced-Security練習問題集
- 試験の準備方法-有効的なGitHub-Advanced-Security的中率試験-ハイパスレートのGitHub-Advanced-Security技術試験 □ ➡ www.goshiken.com □は、□ GitHub-Advanced-Security □を無料でダウンロードするのに最適なサイトですGitHub-Advanced-Security日本語版テキスト内容
- GitHub-Advanced-Securityウェブトレーニング □ GitHub-Advanced-Security認定試験 □ GitHub-Advanced-Security関連日本語内容 □ ▶ GitHub-Advanced-Security ◀の試験問題は□ www.passtest.jp □で無料配信中GitHub-Advanced-Securityウェブトレーニング
- GitHub-Advanced-Security試験問題解説集 □ GitHub-Advanced-Security受験資料更新版 □ GitHub-Advanced-Security練習問題集 □ ⇒ www.goshiken.com ⇐で□ GitHub-Advanced-Security □を検索して、無料でダウンロードしてくださいGitHub-Advanced-Security受験内容
- GitHub-Advanced-Security試験復習赤本 □ GitHub-Advanced-Security受験内容 □ GitHub-Advanced-Security無料試験 □ 最新 ➡ GitHub-Advanced-Security □問題集ファイルは【 www.passtest.jp 】にて検索GitHub-Advanced-Security赤本勉強
- GitHub-Advanced-Security関連日本語内容 □ GitHub-Advanced-Security関連日本語内容 □ GitHub-Advanced-Securityテスト対策書 □ サイト ➡ www.goshiken.com □で ➡ GitHub-Advanced-Security □問題集をダウンロードGitHub-Advanced-Security試験
- 一番優秀なGitHub-Advanced-Security的中率 - 合格スムーズGitHub-Advanced-Security技術試験 | 検証するGitHub-Advanced-Security日本語資格取得 □ “www.topexam.jp”に移動し、（GitHub-Advanced-Security）を検索して、無料でダウンロード可能な試験資料を探しますGitHub-Advanced-Security認定試験
- GitHub-Advanced-Security無料試験 □ GitHub-Advanced-Security赤本合格率 □ GitHub-Advanced-Security日本語版テキスト内容 □ URL □ www.goshiken.com □をコピーして開き、▶ GitHub-Advanced-Security ◀を検索して無料でダウンロードしてくださいGitHub-Advanced-Security赤本合格率
- GitHubのGitHub-Advanced-Security認定試験に楽に受かるコツが何だろう □ ➡ www.japancert.com □を開いて「GitHub-Advanced-Security」を検索し、試験資料を無料でダウンロードしてくださいGitHub-Advanced-Security受験内容
- pixabay.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.intensedebate.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Japancert GitHub-Advanced-Securityダンプの一部を無料でダウンロード: <https://drive.google.com/open?id=1QMA2Ln5VN4NNfIcZ21umolusXD1YgGVg>

