

# 完璧な312-97参考資料 & 合格スムーズ312-97日本語版 サンプル | 最新の312-97日本語版復習資料



コンテンツだけでなくディスプレイでも、312-97テスト準備の設計に最新のテクノロジーを適用しました。結果として、あなたは変化する世界に歩調を合わせ、312-97トレーニング資料であなたの利点を維持することができます。また、重要な知識を個人的に統合し、カスタマイズされた学習スケジュールやTo Doリストを毎日設計できます。最後になりましたが、アフターサービスは、312-97ガイド急流で最も魅力的なプロジェクトになる可能性があります。

ECCouncil 312-97認定資格試験が難しいので、弊社の312-97問題集はあなたに相当する認定資格試験問題集を見つけるし、本当の試験問題の難しさを克服することができます。弊社はECCouncil 312-97認定試験の最新要求に従って関心を持って、全面的かつ高品質な模擬試験問題集を提供します。また、購入する前に、無料で312-97のPDF版デモをダウンロードでき、信頼性を確認することができます。

>> 312-97参考資料 <<

## 信頼的な312-97参考資料一回合格-実地的な312-97日本語版サンプル

312-97試験の質問に協力して、312-97試験に合格し、312-97証明書を正常に取得することをお約束します。以前のお客様に対する最近の調査によると、99%のECCouncilお客様が目標を達成できるため、最終的な目標の達成を支援するお手伝いができると考えています。ベッドサイドには、新しい知識の開発を管理するための高品質の312-97テストガイドがあるため、すべてのEC-Council Certified DevSecOps Engineer (ECDE)学習ポイントをバランスよく把握できます。

## ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) 認定 312-97 試験問題 (Q16-Q21):

### 質問 # 16

(Judi Dench has recently joined an IT company as a DevSecOps engineer. Her organization develops software products and web applications related to electrical engineering. Judi would like to use Anchore tool for container vulnerability scanning and Software Bill of Materials (SBOM) generation. Using Anchore gype, she would like to scan the container images and file systems for known vulnerabilities, and would like to find vulnerabilities in major operating system packages such as Alpine, CentOS, Ubuntu, etc. as well as language specific packages such as Ruby, Java, etc. Which of the following commands should Judi run to scan for vulnerabilities in the image using gype?)

- A. gype < image >.
- B. gype packages < image > --scope all-layers.
- C. gype packages < image >.
- D. gype < image > --scope all-layers.

正解: D

解説:

Grype is a vulnerability scanning tool used to analyze container images and file systems for known vulnerabilities across operating system and application dependencies. The most effective way to perform a comprehensive scan is by running the `grype <image> --scope all-layers` command. This ensures that vulnerabilities are detected across all layers of the container image, not just the final runtime layer. Containers often inherit vulnerabilities from base images or intermediate layers, making full-layer scanning essential. The `packages` subcommand is used for listing detected packages rather than performing vulnerability analysis. Running Grype during the Build and Test stage allows DevSecOps teams to identify vulnerable base images and dependencies early, reducing the risk of deploying insecure containers into production and supporting secure container lifecycle management.

---

#### 質問 # 17

(William Edwards is working as a DevSecOps engineer at SVR Software Solution Pvt. Ltd. His organization develops software products and applications related to digital marketing. William integrated Prisma Cloud with Jenkins to detect threat-intelligence based threat detection. This integration will allow him to scan container images and serverless functions for security issues in the CI/CD pipeline. Which of the following is employed by Prisma Cloud to understand the normal network behavior of each customer's cloud environment to detect network anomalies and zero-day attacks effectively with minimal false positives?.)

- A. Advanced supervised machine learning
- B. Advanced unsupervised data mining
- C. Advanced unsupervised machine learning
- D. Advanced supervised data mining

正解: C

解説:

Prisma Cloud leverages advanced unsupervised machine learning to establish baselines of normal behavior within a customer's cloud environment. By analyzing patterns in network traffic, resource interactions, and workload behavior without relying on labeled training data, it can detect anomalies and potential zero-day attacks with minimal false positives. Supervised approaches require predefined labels and known attack patterns, which limits effectiveness against new or unknown threats. Unsupervised data mining alone lacks the adaptive intelligence provided by machine learning models. Using unsupervised machine learning during the Build and Test stage enables continuous, intelligent security analysis across dynamic cloud-native workloads, supporting proactive threat detection in DevSecOps pipelines.

#### 質問 # 18

(Dave Allen is working as a DevSecOps engineer in an IT company located in Baltimore, Maryland. His team is working on the development of Ruby on Rails application. He integrated Brakeman with Jenkins to detect security vulnerabilities as soon as they are introduced; he then installed and configured Warnings Next Generation Plugin in Jenkins. What will be the use of Warnings Next Generation Plugin to Dave?.)

- A. It will gather and manage the results from Brakeman.
- B. It will inspect TypeScript code for readability, functionality, and maintainability issues.
- C. It will regulate the function of Brakeman.
- D. It will validate Jenkins compiler settings.

正解: A

解説:

The Warnings Next Generation Plugin in Jenkins is designed to collect, aggregate, visualize, and manage static analysis results produced by various tools, including Brakeman. In this scenario, Dave uses Brakeman to scan Ruby on Rails applications for security vulnerabilities. Brakeman generates output files containing findings, and the Warnings Next Generation Plugin parses these results and presents them in a standardized, user-friendly format within Jenkins. This allows teams to track trends, enforce quality gates, and fail builds based on severity thresholds. The plugin does not inspect TypeScript code, validate compiler settings, or control Brakeman's execution logic. Its role is purely to manage and display analysis results. Using this plugin during the Code stage improves visibility into security issues, supports decision-making, and helps enforce security standards across the development lifecycle.

---

#### 質問 # 19

(Lisa Kramer carries an experience of 4 years as a DevSecOps engineer in an IT company. The software development team of her organization has developed a Ruby on Rails web application and would like to find vulnerabilities in Ruby dependencies. Therefore, the team leader of the software development team approached Lisa for help in this regard. Which of the following SCA tool should Lisa use to detect vulnerabilities in Ruby dependencies?)

- A. Bandit.
- B. Retire.js.
- C. Tenable.io.
- **D. Bundler-Audit.**

**正解: D**

解説:

Bundler-Audit is an SCA tool designed specifically for Ruby applications. It analyzes the Gemfile and Gemfile.lock to identify dependencies and checks them against known vulnerability databases. Bandit is intended for Python code analysis, Retire.js targets JavaScript libraries, and Tenable.io focuses on infrastructure-level vulnerabilities. By using Bundler-Audit during the Code stage, DevSecOps teams can detect vulnerable Ruby gems early and ensure that only secure dependencies are used. This reduces the risk of exploiting known vulnerabilities in third-party libraries and supports secure dependency management throughout the development lifecycle.

---

#### 質問 # 20

(Alex Hales recently joined TAVR Software Solution Pvt. Ltd. As a DevSecOps engineer. To automatically detect security loopholes in the web applications while building and testing them, he integrated OWASP ZAP DAST Plugin with Jenkins. How can Alex uniquely identify every build in the project?.)

- **A. By specifying a file name followed by \${Build\_ID} in Post-build Actions tab.**
- B. By specifying a file name followed by \${zap\_scan} in Post-build Actions tab.
- C. By specifying a file name followed by \${Profile\_ID} in Post-build Actions tab.
- D. By specifying a file name followed by \${ZAPROXY\_HOME} in Post-build Actions tab.

**正解: A**

解説:

Jenkins automatically assigns a unique identifier to each build using the environment variable BUILD\_ID. When integrating OWASP ZAP with Jenkins, appending \${BUILD\_ID} to output filenames or reports ensures that every scan result corresponds to a specific build execution. This avoids overwriting previous reports and allows traceability between build artifacts and security findings. Variables such as \${ZAPROXY\_HOME} refer to installation paths, not build uniqueness, while \${Profile\_ID} and \${zap\_scan} are not standard Jenkins variables for uniquely identifying builds. Using \${BUILD\_ID} supports better auditing, historical analysis, and correlation between detected vulnerabilities and the exact build in which they were found, which is critical during the Build and Test stage of a DevSecOps pipeline.

---

#### 質問 # 21

.....

当社ECCouncilの312-97学習教材は、複数のエクスペリエンスモードを提供できます。3つの主要なモードから選択できます: PDF、ソフトウェア、オンライン。まず、JapancertPDFバージョンは印刷可能です。第二に、312-97試験問題のソフトウェアバージョンでは、実際の試験環境をシミュレートして、試験体験をより鮮明にできます。第三に、オンライン版はすべてのWebブラウザをサポートしているため、すべてのオペレーティングシステムで動作します。また、312-97学習教材は、よりリラックスした学習環境で312-97試験に合格するのに役立ちます。

**312-97日本語版サンプル:** <https://www.japancert.com/312-97.html>

ECCouncil 312-97参考資料 試験に失敗した場合、ただ不合格の証明書をスキャンしてこちらに送ることが必要です、Japancert 312-97日本語版サンプルが提供した問題と解答はIT領域のエリートたちが研究して、実践して開発されたものです、テスト312-97認定の取得は、学習プロセスの目標を達成するために必要であり、労働者のた

めに働いており、開発のためのより広いスペースを提供できるより多くの資格を持っています、ECCouncil 312-97参考資料 それは情報の時代です、あなたの予算が限られている場合に完全な問題集を必要としたら、JapancertのECCouncilの312-97試験トレーニング資料を試してみてください、とても幸運！

途端に頬を膨らませて、仏頂面で俺を睨み付ける、何でも先生のおっしゃるとおりにい312-97たしますよ草薙はポケットのキーを探りながら、スカイラインに向かって歩きだした、試験に失敗した場合、ただ不合格の証明書のスキャンしてこちらに送ることが必要です。

## 312-97試験の準備方法 | 権威のある312-97参考資料試験 | 信頼的なEC-Council Certified DevSecOps Engineer (ECDE)日本語版サンプル

Japancertが提供した問題と解答はIT領域のエリートたちが研究して、実践して開発されたものです、テスト312-97認定の取得は、学習プロセスの目標を達成するために必要であり、労働者のために働いており、開発のためのより広いスペースを提供できるより多くの資格を持っています。

それは情報の時代です、あなたの予算が限られている場合に完全な問題集を必要としたら、JapancertのECCouncilの312-97試験トレーニング資料を試してみてください。

- 312-97学習体験談 □ 312-97日本語対策 □ 312-97日本語的中対策 ◀ 《 www.passtest.jp 》には無料の ➡ 312-97 □ 問題集があります312-97資格問題対応
- 312-97日本語版問題集 □ 312-97日本語版問題集 □ 312-97独学書籍 □ 「 312-97 」の試験問題は「 www.goshiken.com 」で無料配信中312-97模擬試験問題集
- 検証する312-97参考資料試験-試験の準備方法-ハイパスレートの312-97日本語版サンプル □ 《 www.mogixam.com 》サイトにて最新✓ 312-97 □ ✓ □ 問題集をダウンロード312-97資格問題対応
- 最高の312-97参考資料 - 合格スムーズ312-97日本語版サンプル | 実用的な312-97日本語版復習資料 EC-Council Certified DevSecOps Engineer (ECDE) □ ➡ 312-97 □ □ □ の試験問題は [ www.goshiken.com ] で無料配信中312-97合格体験記
- 312-97試験の準備方法 | 最高の312-97参考資料試験 | 真実的なEC-Council Certified DevSecOps Engineer (ECDE)日本語版サンプル □ { www.japancert.com } で ▶ 312-97 ◀ を検索して、無料で簡単にダウンロードできます312-97日本語的中対策
- 312-97日本語版復習資料 !! 312-97独学書籍 □ 312-97日本語版復習指南 □ ✓ www.goshiken.com □ ✓ □ で 「 312-97 」を検索して、無料で簡単にダウンロードできます312-97試験勉強過去問
- 312-97参考書勉強 □ 312-97日本語版復習資料 □ 312-97日本語的中対策 □ ➤ 312-97 □ を無料でダウンロード“ www.xhs1991.com ”で検索するだけ312-97合格体験記
- 312-97独学書籍 □ 312-97日本語版問題集 □ 312-97無料試験 □ ウェブサイト ▶ www.goshiken.com ◀ を開き、【 312-97 】を検索して無料でダウンロードしてください312-97試験勉強過去問
- ハイパスレート-権威のある312-97参考資料試験-試験の準備方法312-97日本語版サンプル □ ➡ 312-97 □ □ を無料でダウンロード [ www.shikenpass.com ] ウェブサイトを入力するだけ312-97必殺問題集
- ハイパスレート-権威のある312-97参考資料試験-試験の準備方法312-97日本語版サンプル □ ✓ www.goshiken.com □ ✓ □ で使える無料オンライン版 ➡ 312-97 □ の試験問題312-97日本語版復習指南
- 312-97必殺問題集 □ 312-97無料試験 □ 312-97学習体験談 □ { www.mogixam.com } に移動し、□ 312-97 □ 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312-97日本語版復習指南
- www.stes.tyc.edu.tw, codifysolutions.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.hulkshare.com, www.stes.tyc.edu.tw, yiwnhua.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes