Google Cloud

Professional Security Operations Engineer

認定試験ガイド

Google Cloud Certified Professional Security Operations Engineer は、ワークロード、エンドポイント、インフラストラクチャに対するセキュリティ上の脅威を検出、監視、分析、調査し、対応します。Google Cloud リソースを使用して企業環境を保護する役割であり、検出ルールの作成、ログの優先順位付けと取り込み、オーケストレーション、対応の自動化に精通していることが求められます。さらに、脅威の検出と対応のためのセキュリティ ポスチャーと脅威インテリジェンスの活用経験も求められます。

この試験では、Google Security Operations（SecOps）と Security Command Center（SCC）でのタスク実行に関する知識を評価します。これらのプラットフォームの詳細については、Google SecOps のドキュメントと SCC のドキュメントをご覧ください。

セクション 1: プラットフォーム運用（試験内容の約 14%）

1.1 検出と対応の強化。以下のような点を考察します。

- テレメトリー ソース（Security Command Center（SCC）、Google Security Operations（SecOps）、GTI、Cloud IDS など）を優先順位付けして、企業環境内でインシデントや構成ミスを検出する
- セキュリティ アーキテクチャの複数のツール（SCC、Google SecOps、GTI、Cloud IDS、サードパーティのダウンストリーム システムなど）を統合して検出機能を強化する
- 一連の要件に基づいて、重複する機能を持つツールの使用を正当化する
- 既存のツールの有効性を評価して、カバレッジのギャップを特定し、潜在的な脅威を軽減する
- 自動化やクラウドベースのツールを評価して、既存の検出や対応プロセスを強化する

1.2 アクセスの構成。以下のような点を考察します。

- セキュリティツール（SCC、Google SecOps など）にユーザーとサービスアカウントの認証を構成する
- IAM ロールと権限を使用した機能アクセスのためのユーザーとサービス アカウントの認証を構成する

- IAM ロールと権限を使用してデータアクセスにユーザーとサービス アカウントの認証を構成する
- ソリューションに監査ログ（Cloud Audit Logs、データアクセス ログなど）を構成して分析する
- セキュリティ ツール（サービス アカウント、API キー、SCC、Google SecOps、GTI など）内で自動化に API アクセスを構成する
- Workforce Identity 連携を使用して ID をプロビジョニングする

セクション **2:** データ マネジメント（試験内容の約 **14%**）

2.1 セキュリティ ツールへのログの取り込み。以下のような点を考察します。

- セキュリティ ツール（SCC、Google SecOps など）内でのデータの取り込み方法を決定する
- セキュリティ ツール（SCC、Google SecOps など）内で取り込みツールまたは機能を構成する
- セキュリティ ツール（SCC Event Threat Detection、Google SecOps など）内で自動ソースをはじめ、検出と対応に必要なログを評価する
- Google SecOps におけるデータ取り込み用のパーサーを評価する
- Google SecOps でパーサーの変更または拡張機能を構成する
- Google SecOps のログソースからデータを正規化する手法を評価する
- データの取り込み用の新しいラベルを評価する
- ログと取り込みにかかる費用を管理する

2.2 ユーザー、アセット、エンティティのコンテキストにおけるベースラインの特定。以下のような点を考察します。

- 企業環境における関連する脅威インテリジェンス情報を特定する
- イベントとエンティティ データのログソース（Cloud Audit Logs、Active Directory の組織のコンテキストなど）を区別する
- 拡充のため、エイリアシング フィールドを使用して、イベントとエンティティ データの一致を評価する

セクション **3:** 脅威ハンティング（試験内容の約 **19%**）

3.1 環境全体での脅威ハンティングの実行。以下のような点を考察します。

- 異常なアクティビティを特定するため、環境ログ全体を検索するクエリを開発する
- ユーザーの行動を分析して異常なアクティビティを特定する

- Google Cloud ツール（ログ エクスプローラ、ログ分析、BigQuery、Google SecOps など）を使用してネットワーク、エンドポイント、サービスを調査し、脅威パターンやセキュリティ侵害インジケータ（IOC）を特定する
- インシデント対応チームと協力して、環境内のアクティブな脅威を特定する
- 動作、脅威インテリジェンス、ポスチャー、インシデント データ（SCC、GTI など）に基づいて仮説を立てる

3.2 脅威ハンティングへの脅威インテリジェンスの活用。以下のような点を考察します。

- 履歴ログ内で IOC を検索する
- 脅威インテリジェンスとリスク評価（GTI、検出ルール、SCC の有害な組み合わせなど）を使用して、新しい攻撃パターンと手法をリアルタイムで特定する
- エンティティ リスクスコアを分析して異常な動作を特定する
- 過去のイベントデータを新たに強化されたログ（Google SecOps ルールエンジン、BigQuery、Cloud Logging など）と比較して RetroHunt を実行する
- 脅威インテリジェンス（GTI、検出ルールなど）を使用して潜在的な脅威をプロアクティブに検索する

セクション **4:** 検出エンジニアリング（試験内容の約 **22%**）

4.1 リスクを検出して脅威を特定するメカニズムの開発と実装。以下のような点を考察します。

- 脅威インテリジェンスをユーザーやアセット アクティビティごとに調整する
- ログとイベントを分析して異常なアクティビティを特定する
- 検出ルールとさまざまなタイムラインにわたる検索を使用して、不審な行動パターンを評価する
- リスク値（Google SecOps 参照リストなど）を使用した検出ルールを設計してリスク プロファイルに一致する脅威を特定する
- アセットやユーザーの異常な行動を検出し、その検出結果にリスク値を割り当てる（Google SecOps リスク分析、キュレーテッド検出のルールなど）
- 環境内のポスチャーやリスク プロファイルの変化を検出するための検出ルールを設計する（SCC Security Health Analytics（SHA）、SCC のポスチャー管理、Google SecOps など）
- さまざまな方法（YARA-L ルールの作成、ダッシュボードなど）を使用して、脅威インテリジェンス ソースに表示されない新しいまたは低頻度のプロセス、ドメイン、IP アドレスを特定する
- 検出ルール内でエンティティ / コンテキスト データをどのように使用して精度を向上させるかを評価する（Google SecOps エンティティ グラフなど）
- IOC 用の SCC Event Threat Detection カスタム検出機能を構成する

4.2 検出に必要な脅威インテリジェンスの活用。以下のような点を考察します。

- IOC のリスクレベルに基づいてアラートをスコアリングする
- 最新の IOC を使用して、取り込んだセキュリティ テレメトリー内を検索する
- 繰り返し発生するアラートの頻度を測定し、誤検知を特定して削減する

セクション 5: インシデント対応 (試験内容の約 21%)

5.1 セキュリティ インシデントの封じ込めと調査。以下のような点を考察します。

- フォレンジック画像やアーティファクトをはじめとするインシデントの範囲に関する証拠を収集する
- セキュリティ ツール（SCC、Google SecOps など）を使用してインシデントに関連するアラートを観察して分析する
- セキュリティ ツール（ログ エクスプローラ、ログ分析、BigQuery、Cloud Logging、Cloud Monitoring など）を使用してインシデントの範囲を分析する
- 検出と長期的な修復作業を目的として他のエンジニアリング チームと連携する
- 影響を受けるサービスやプロセスを分離し、さらなる被害や攻撃の拡大を防ぐ
- フォレンジック分析（ハッシュ、IP、URL、バイナリなど）に基づいて特定されたアーティファクトを分析する（GTI）
- セキュリティ ツール（SCC、Google SecOps SIEM など）を使用して根本原因分析を実行する

5.2 対応ハンドブックの構築、実装、使用。以下のような点を考察します。

- 自動化に適した対応手順を決定する
- 脅威プロファイルに基づいて価値の高い拡充に優先順位を付ける
- ハンドブックで活用できる適切な統合を評価する
- 最近のインシデントから新たに特定された攻撃パターンに対応するための新しいプロセスを設計する
- 現在の実装（Google SecOps SOAR など）のギャップに基づいて新しいオーケストレーションと自動化ハンドブックを推奨する
- アナリストや関係者にインシデントを通知するメカニズムを実装する

5.3 ケース管理ライフサイクルの実装。以下のような点を考察します。

- 適切な対応段階にケースを割り当てる
- ケースのエスカレーションに効率的なワークフローを実装する
- ケースの引き継ぎについての有効性を評価する

セクション **6:** オブザーバビリティ（試験内容の約 **10%**）

6.1 分析情報を提供するダッシュボードとレポートの構築と保守。以下のような点を考察します。

- 主要なセキュリティ分析（指標、KPI、トレンドなど）を特定する
- セキュリティ テレメトリー、取り込み指標、検出、アラート、IOC（Google SecOps SOAR、セキュリティ情報およびイベント管理、Looker Studio など）を表示するためのダッシュボードを実装する
- レポート（Google SecOps SOAR、セキュリティ情報およびイベント管理など）を生成してカスタマイズする

6.2 ヘルス モニタリングとアラートの構成以下のような点を考察します。

- ヘルス モニタリングとアラートのための重要な指標を特定する
- 指標を一元管理するダッシュボードを作成する
- 特定の指標のしきい値を設定したアラートを作成する
- Google Cloud ツール（Cloud Monitoring など）を使用して通知を設定する
- Google Cloud ツール（Cloud Logging など）を使用して健全性の問題を特定する
- サイレント ソースの検出を構成する