ORACLE

Oracle Cloud Guard

Oracle Cloud Infrastructureでのクラウド・セキュリティ体制管理

2020年9月、バージョン1.0

公開

本書の目的

本書では、Oracle Cloud Infrastructureの機能および強化点の概要を説明しています。本書は、ITプロジェクトの計画を支援することのみを目的としています。

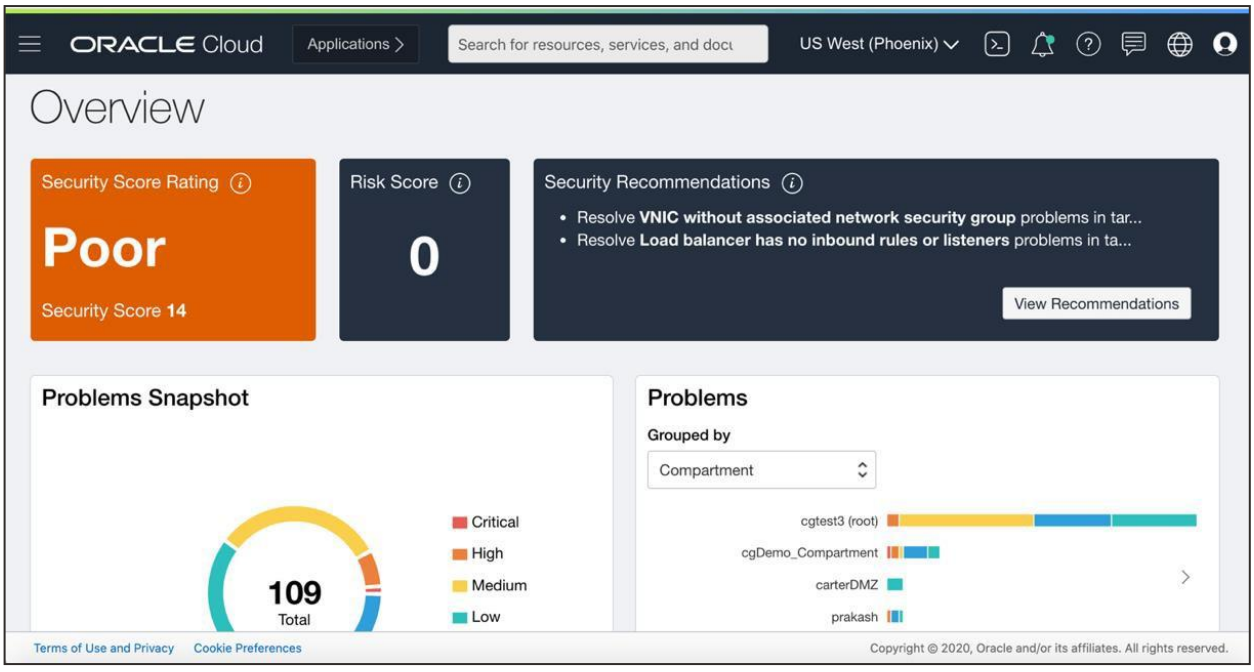
免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書と本文書に含まれる情報は、オラクルの事前の書面による同意なしに、公開、複製、再作成、またはオラクルの外部に配布することはできません。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書は情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料にするものでもありません。本書に記載されている機能の開発、リリースおよび時期については、オラクルの裁量により決定されます。製品アーキテクチャの性質上、コードが大幅に不安定化するリスクなしに、本書に記載されているすべての機能を安全に含めることができない場合があります。

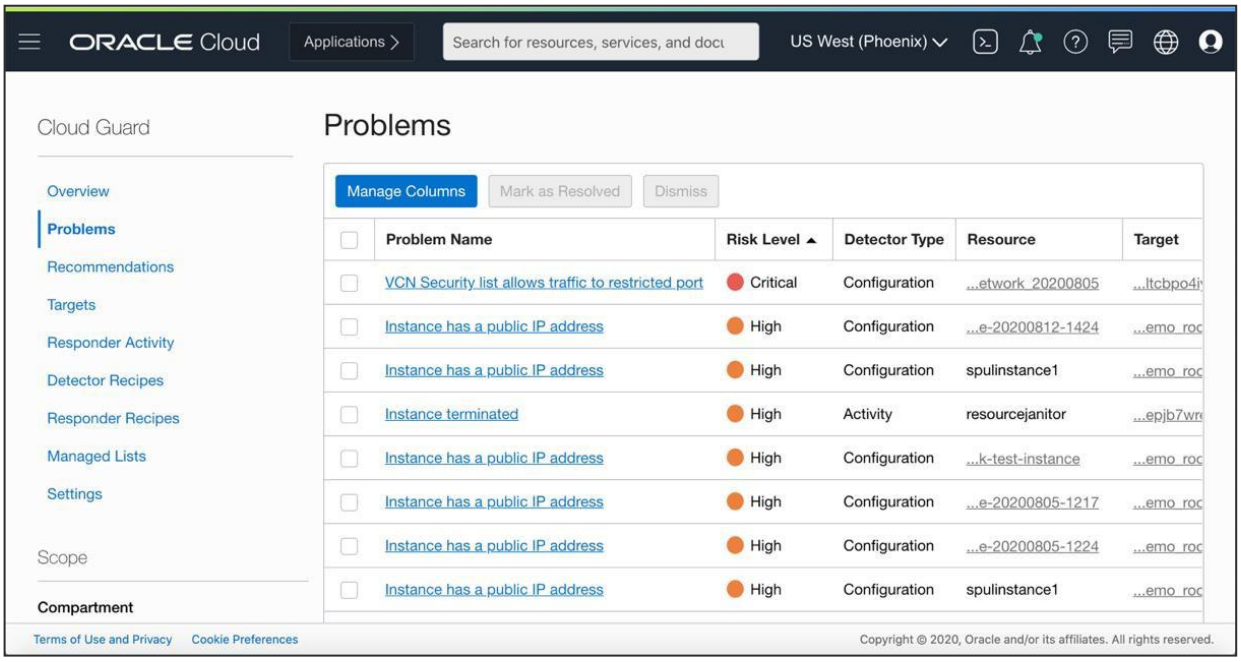
クラウドでの不適切なリソース設定やセキュアでないアクティビティは、セキュリティ・プロフェッショナルにとってきわめて困難な問題になります。クラウド・リソースに関するクラウド・テナンシーの設定が不適切な場合、オブジェクト・ストレージ・バケットへのパブリック・アクセスが可能になる、データ・ストレージが暗号化されない、機密ポートがインターネットに公開されるなど、さまざまな問題が生じる可能性があります。クラウド内でのユーザーと管理者の行動も懸念の対象となります。クラウド・インフラストラクチャにおいて、セキュアではないアクティビティを検出するのは困難です。これらは単純な検出ルールの枠を越えることが多く、認証済みユーザーによって引き起こされる場合もあるからです。侵入、偵察、エクスプロイト、権限昇格、窃取など、サイバー・キル・チェーンのさまざまな段階が、セキュアではないアクティビティの原因となり得ます。

Oracle Cloud Infrastructure Cloud Guardは、不適切なリソース設定とセキュアでないアクティビティを検出するクラウド・セキュリティ・サービスです。Cloud Guardは、ログおよびイベントのアグリゲータとして機能し、すべての主要なOracle Cloud Infrastructureサービス（コンピュート、ネットワーキング、ストレージなど）と直接統合することで、役に立つ結果を提供します。Cloud Guardが持つ柔軟性により、セキュリティの問題に対して手動で対策を取ることも、条件付き演算子を使用して自動化することもできます。

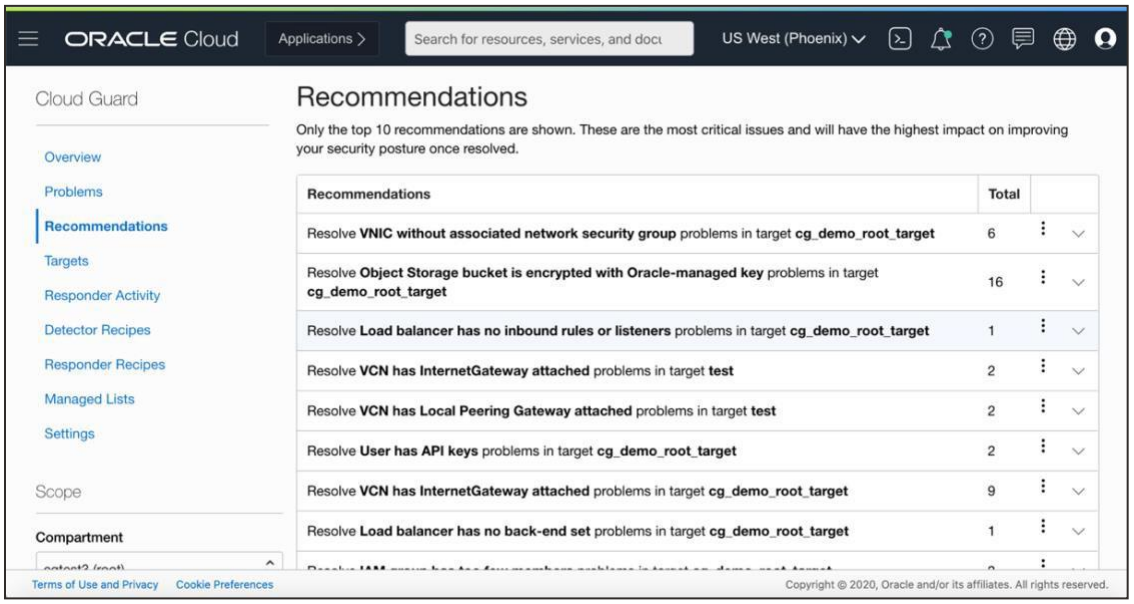


Cloud GuardのOverviewでは、OCIテナンシー内の総合的なクラウド・セキュリティ対策状況を単一ビューで確認できます。ダッシュボードには、さまざまな分析機能が多数搭載されており、セキュリティ担当者がクラウド・セキュリティの問題を識別、トリアージ、優先順位付けするのに役立ちます。Cloud Guardには、クラウド・セキュリティ・スコアカードの使用が含まれているため、管理者は長期的にリスクを管理するための定量的な基準が得られます。さらに、セキュリティ課題（Cloud Guardでは問題と呼ばれる）には自動的に重大度が割り当てられ、ダッシュボード内でコンパートメント/リージョン/リソース・タイプ別にグループ化できます。

Cloud Guardで特定された課題は問題と呼ばれます。従来のセキュリティ・オペレーション・センターのワークフローでセキュリティ課題を管理するのと同じように、Cloud Guardコンソールに問題が表示されます。問題はキュー内にリスト表示され、不適切なリソース設定またはセキュアでないアクティビティのどちらかに分類されます。セキュリティ・アナリストはある問題をドリルダウンし、リソース名、リソース・タイプ、コンパートメント、検出時刻などの詳細情報を利用して調査を進めることができます。リソース識別子を使用して一意に識別された問題は、修正、解決済みとしてマーク、却下のいずれかの対応を取ることができます。コンプライアンス・レポートのユースケースでは、クラウド・ガードは、誤って構成されたリソースに関連する問題をCenter for Internet Security (CIS)ベンチマークにマップします。

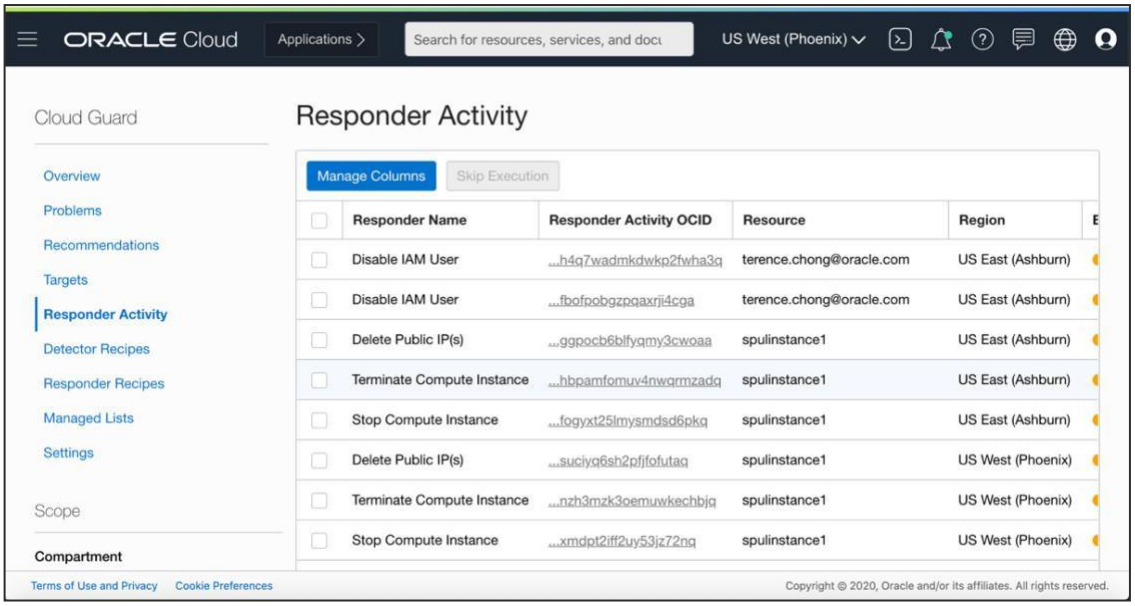


セキュリティに関するオラクルの専門知識が組み込まれたCloud Guardでは、一般的なクラウド・セキュリティ課題を検出する設定不要のレシピ（ディテクタ・レシピ）がエンドユーザーに提供され、修正プロセス（レスポンダ・レシピ）を自動化できます。Cloud Guardディテクタ・レシピは、複製して当該リソースに適した入力設定で変更することができます。複製したレシピは有効化または無効化でき、異なる重大度を課題に適用できます。Cloud Guardディテクタ・レシピは、時間、システム・バージョン、ユーザー、タグ、IPアドレス・メタデータ、リソース識別子に基づくルールベースの条件を提供しています。オラクルが管理するレシピにはルールが追加されますが、デフォルト設定では、これらの新規ルールも複製されたレシピに表示されます。こうすることで、Cloud Guardの対象となるセキュリティ課題が増えて範囲が拡大された場合も、顧客にそれが引き継がれます。修正を自動化するレスポンダ・レシピは、対応時間のギャップを埋め、セキュリティ・プレイブックのテーマ（パブリック・アクセスの削除、ユーザーの無効化、インスタンスの停止、APIキーのローテーション、情報セキュリティ・コミュニケーション・チャネルへのイベント通知の送信など）を取り込むことができます。このように、Cloud Guardは、セキュリティ組織の拡大に役立つクラウド検出/対応フレームワークを提供します。



Cloud Guardは、Oracle Cloud Infrastructure上のマネージド・クラウド・サービスに関するログとイベントを集計するだけでなく、Oracle Cloud Infrastructure全体からメタデータと脅威インテリジェンス・データを取り込んで、特定のクラウド・セキュリティ攻撃タイプに関連付けることができます。たとえば、クラウド・テナンシー内のアカウントを侵害した攻撃者は、居場所を隠すためにコマンド&コントロール・サーバーやTorプロキシに関連付けられたIPアドレスを使用することがあります。Cloud Guardはネットワークベースの脅威インテリジェンス・データを取り込んでいるため、疑わしいIPアドレスからのセキュアでないアクティビティを検出し、互いに関連付けることができます。

セキュリティ運用担当者はレスポンダを使用し、該当するセキュリティ・プレイブックの指定に従ってCloud Guard内の問題を修正できます。特定のタイプの問題が検出された場合は、レスポンダを実行することで平均応答時間を短縮できます。レスポンダは基本的に、イベント基準（問題のタイプ）に基づいて自動的にトリガーされるサーバーレス・コンピュート機能です。Cloud Guardでは、管理者が手動で問題を修正できますが、自動的に修正すると、アナリストがより高度なクラウド・セキュリティの問題に集中できるようになります。



Cloud Guardは、平均対応時間を短縮し、セキュリティ・オペレーション・センターを拡大するために必要なクラウド検出/対応フレームワークを提供します。Cloud GuardはOCIテナンシー内にすばやくデプロイでき、組み込まれたセキュリティの知見を追加設定なしで利用できます。Cloud Guardを今すぐお試しください。Cloud GuardはOracle Cloud Infrastructureの商用リージョンで利用できます。

詳しくは、Oracle Cloud Guardを参照してください。Oracle Cloudのトライアルを無料でお試しいただけます。

Connect with us

+1.800.ORACLE1までご連絡いただくか、**oracle.com**をご覧ください。北米以外の地域では、**oracle.com/contact**で最寄りの営業所をご確認いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle