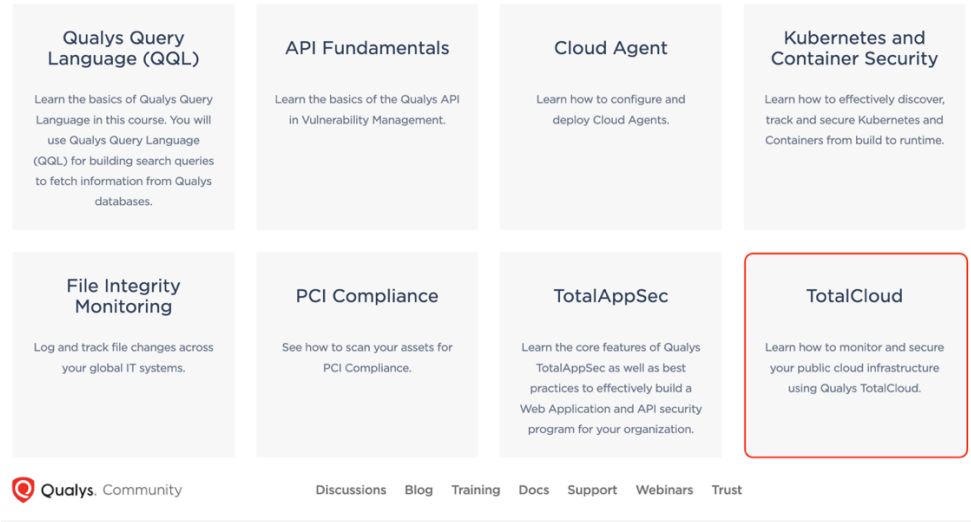
2025 年 10 月

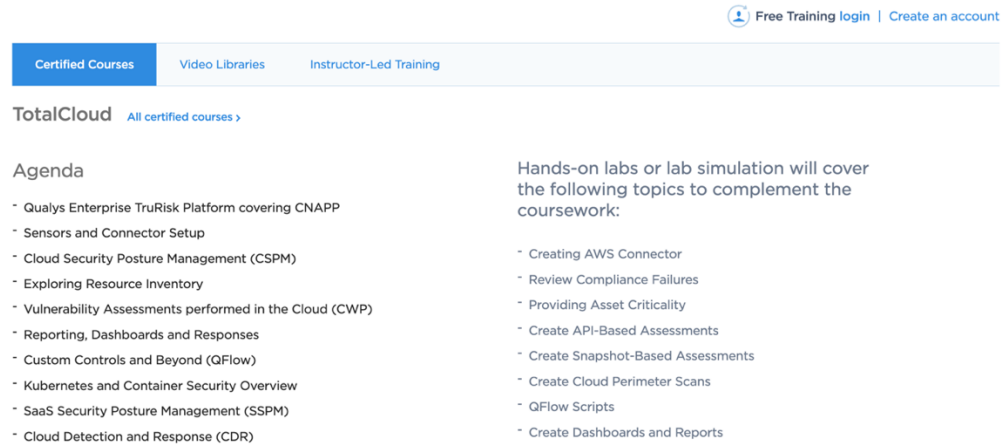
Total Cloud トレーニングガイド

はじめに

本資料は Qualys トレーニングサイトの TotalCloud の学習をより深く理解するための日本語ドキュメントとなります。下記サイトよりフリートレニングにサインアップいただき、TotalCloud のトレーニングをスタートしてください。

https://www.qualys.com/training/





TotalCloud の成功に不可欠です。

1. プラットフォームを理解する
2. センサーの導入方法を理解する
3. クラウド資産を整理する方法を理解する
4. クラウドインベントリを評価する方法を理解する
5. レポートを理解する
6. クラウドインベントリのセキュリティギャップを修復する方法を理解する

スコープ

セキュリティポリシーはありますか? どの資産を最優先にしていますか? どの脆弱性と構成のギャップが最優先ですか? 組織が満たさなければならないコンプライアンス要件はありますか? スキャナアプライアンスを展開する場所を決定するのに役立つネットワーク図はありますか?
どの資産とどの脆弱性が最優先事項であるかを理解することは、Qualys のオンボーディングに取り組む際の行動に役立ちます。
Qualys TruRisk は、脆弱性の優先順位付けを自動化するのに役立ちます。脆弱性の重大度と、ランサムウェア、ラテラルムーブメント、ゼロデイなどに関連する悪用可能性などの追加のリスク要因が考慮されます。また、資産の重要性を考慮し、内部資産よりも外部資産を重視します。これにより、どの資産が優先度が高いか、どの資産が低いかを定義し、これらすべてを変数として使用して TruRisk スコアを計算できます。
繰り返しになりますが、この会話は 3 分間のビデオよりも大きいです。最終的に、組織は、脆弱性や構成のギャップに関して、何を優先し、修復のために定義する SLA について合意する必要があります。

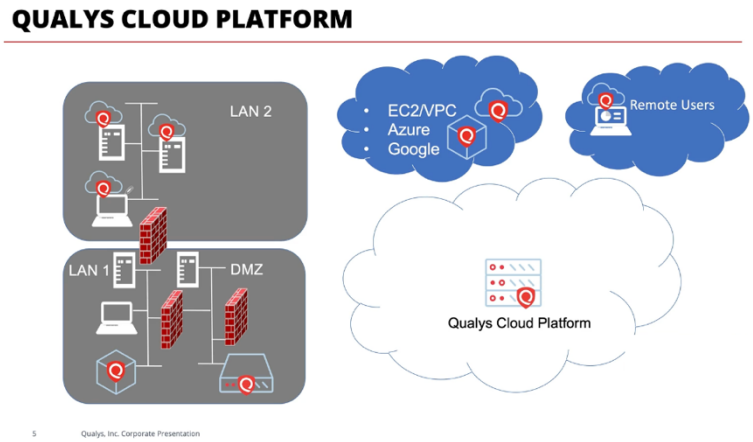
Qualys Cloud Platform の紹介

データがネットワーク内と Qualys プラットフォームにどのように流れるかを理解します。
Cloud Scanner、内部 Scanner Appliance、Cloud Agent など、いくつかのタイプのセンサーを使用します。

クラウドスキャナー:これらは、「攻撃者の視点」でアセットデータを取得するのに役立ちます。 これらを使用して、パブリック IP アドレスをスキャンし、リモート攻撃態勢を可視化します。

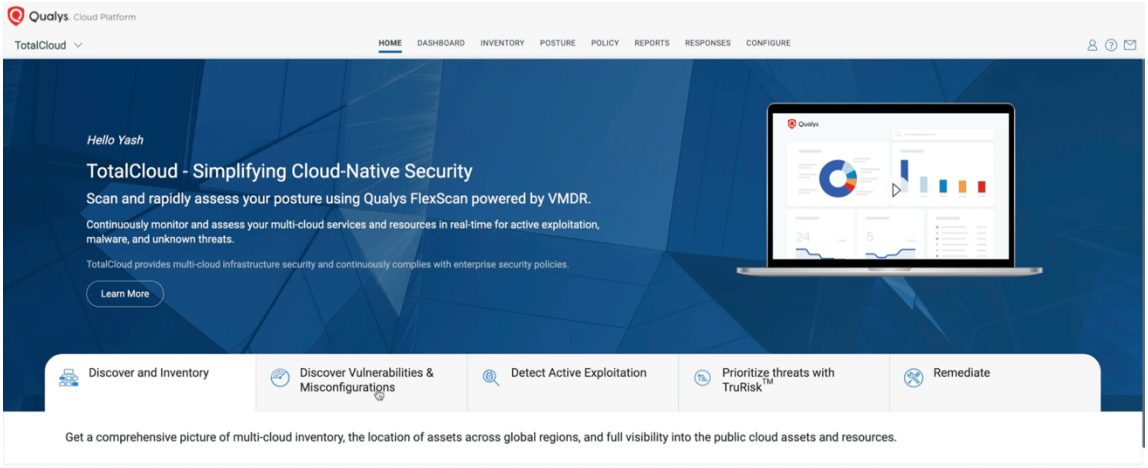
内部スキャナアプライアンス:これらは、内部資産の可視性を高めるのに役立ちます。

クラウドエージェント:脆弱性データを収集する最も効率的な方法(パッチ管理を使用している場合はパッチを適用します)。

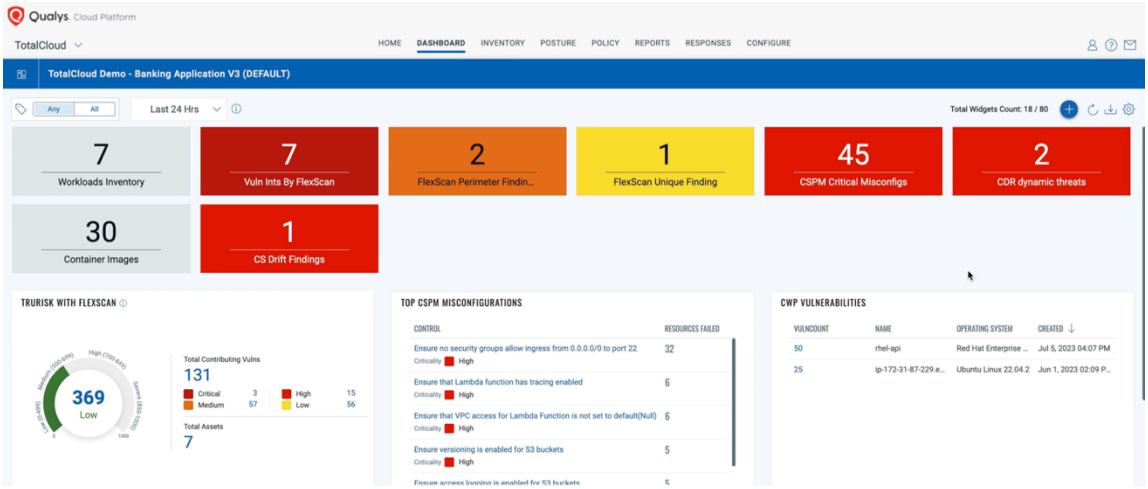


Qualys ユーザー インターフェイス 序章

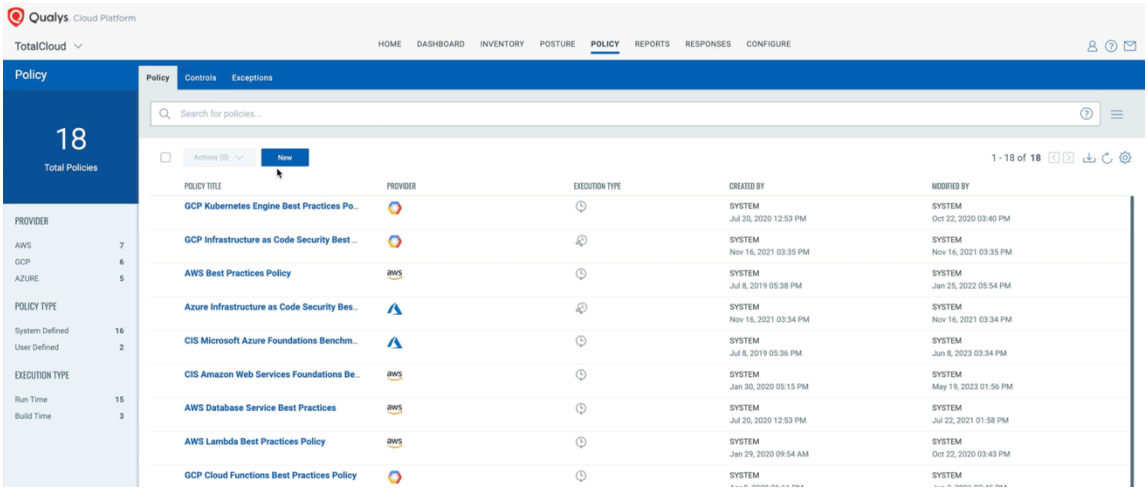
まずはじめに UI の基本を理解します。 以下は TotalCloud の Home ページとなります。



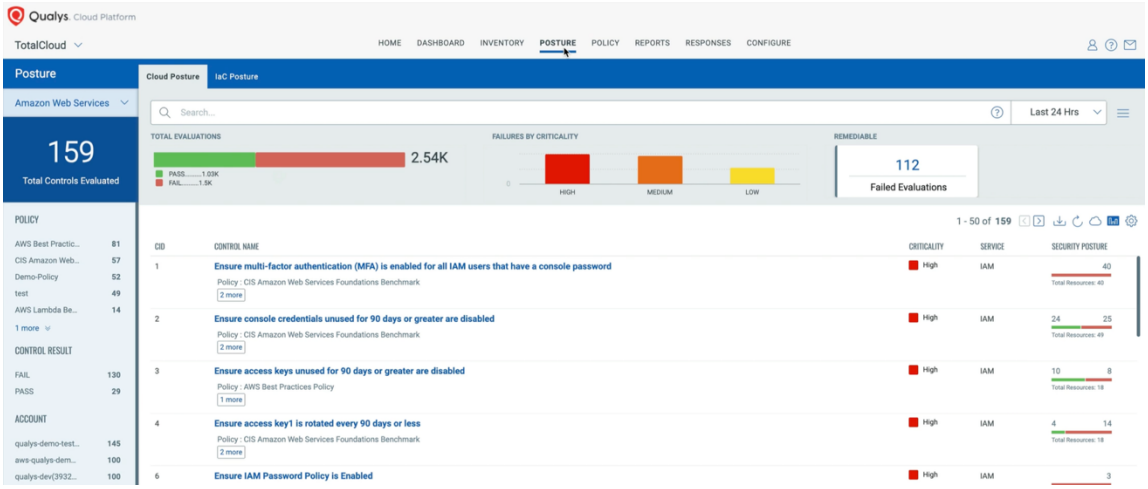
以下は TotalCloud のダッシュボードとなります。



以下はポリシーページです。

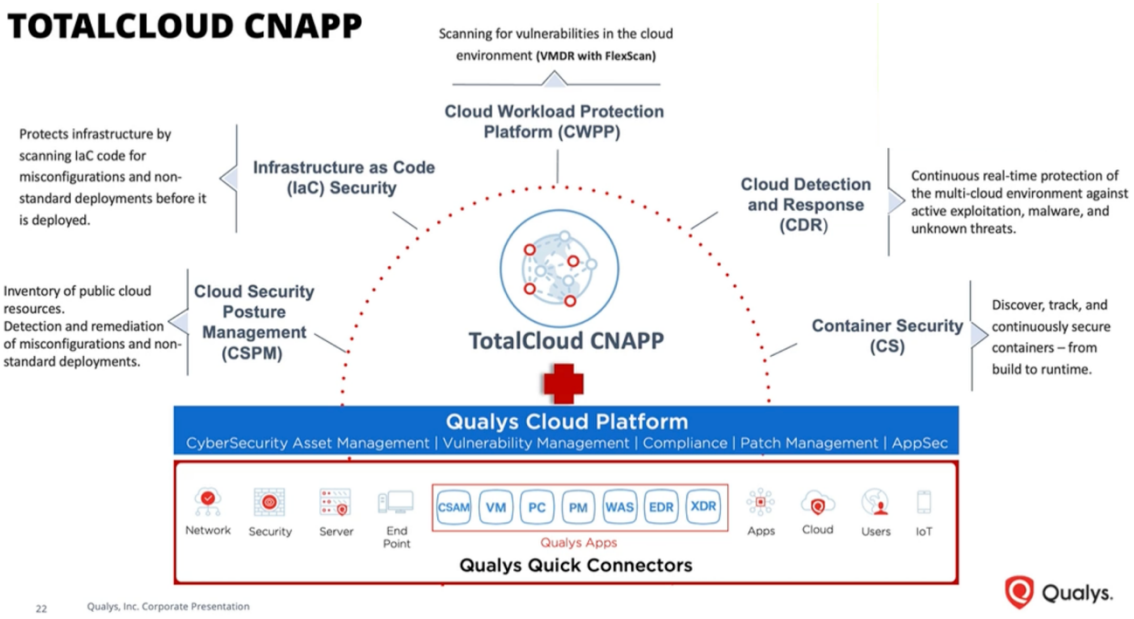


以下はポスチャー結果となります。



CNAPP と TotalCloud

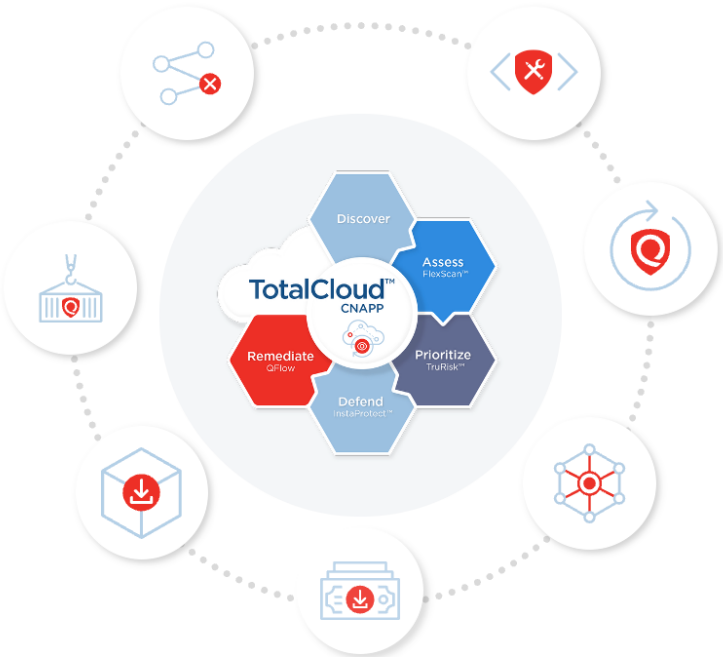
クラウドネイティブ アプリケーション保護プラットフォーム（CNAPP）は、クラウド ネイティブ アプリケーションに包括的な保護を提供するために複数のソリューションを統合することの重要性を強調しています。



Qualys TotalCloud は、クラウドセキュリティポスチャー管理(CSPM)、コードとしてのインフラストラクチャ(IaC)セキュリティ、クラウドワークロード保護(CWPP)、クラウド検出と対応(CDR)、コンテナセキュリティ(CS)を同じQualys プラットフォームから統合して提供することで、クラウドネイティブのアプリとインフラストラクチャを包括的に保護します。

このレッスンでは、クラウドネイティブアプリケーション保護プラットフォーム *(CNAPP)* と *TotalCloud* について学習しました。

TotalCloud のライフサイクル

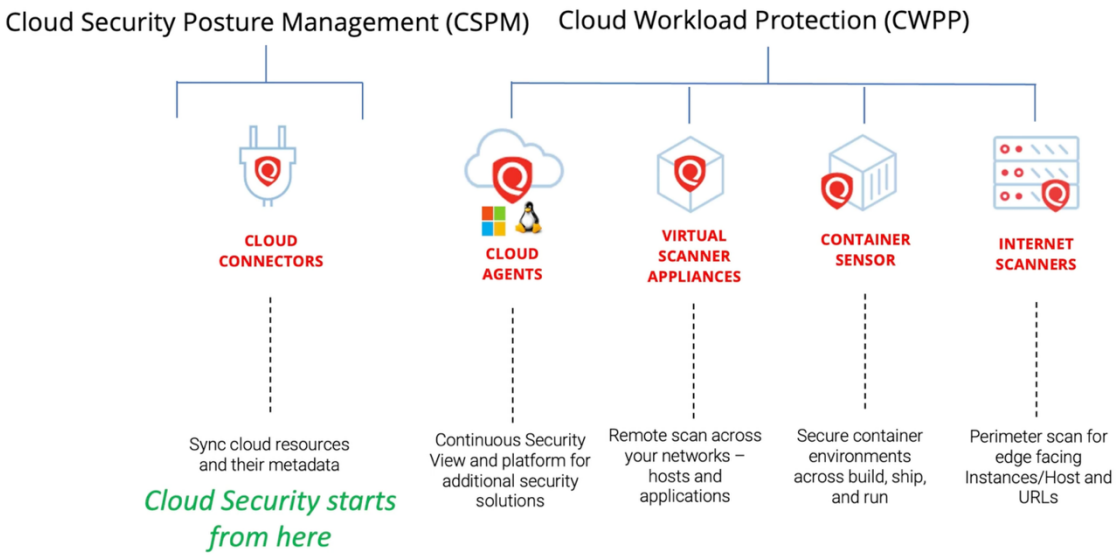


1. **検出(Discover)** - Qualys コネクタを設定して、クラウド環境内のリソースの検出を開始します。コネクタはクラウドアカウントと Qualys をリンクし、Qualys アプリケーションが環境から必要なデータを取得できるようにします。
2. **評価(Access)** - Qualys は、さまざまな種類のスキャナーを容易に使いやすく管理できるテクノロジーを開発しました。これを FlexScan と呼びます。FlexScan により、TotalCloud は、一時的なインスタンスや一時停止中のインスタンス、長時間実行されるワークロードのスキャン、高速スキャンからディープスキャンまで、あらゆるユースケースに対応できます。
3. **優先順位付け(Prioritize)** - このフェーズの主な目的は、TruRisk による重大な脆弱性のコンテキストベースの優先順位付けにより、最も重要な問題に対処することです。脆弱性評価に必要なデータは、Qualys コネクタ、スキャナアプライアンス、またはエージェントの組み合わせから取得できます。
4. **防御(Defend)** – Qualys Cloud Detection and Response (CDR) を活用し、アクティブなエクスプロイト、マルウェア、未知の脅威からマルチクラウド環境を継続的にリアルタイムで保護します。
5. **修復(Remediate)** – Qualys クラウドプラットフォームに組み込まれた修復ツールと機能を活用し、優先度の高い脆弱性を修復します。

資料

- TotalCloud Datasheet
- Blog: TotalCloud and CloudView Integration
- Cloud Security Posture Management
- IaC Security
- Cloud Workload Protection
- Cloud Detection and Response
- Container Security

クラウドセキュリティのための Qualys センサー

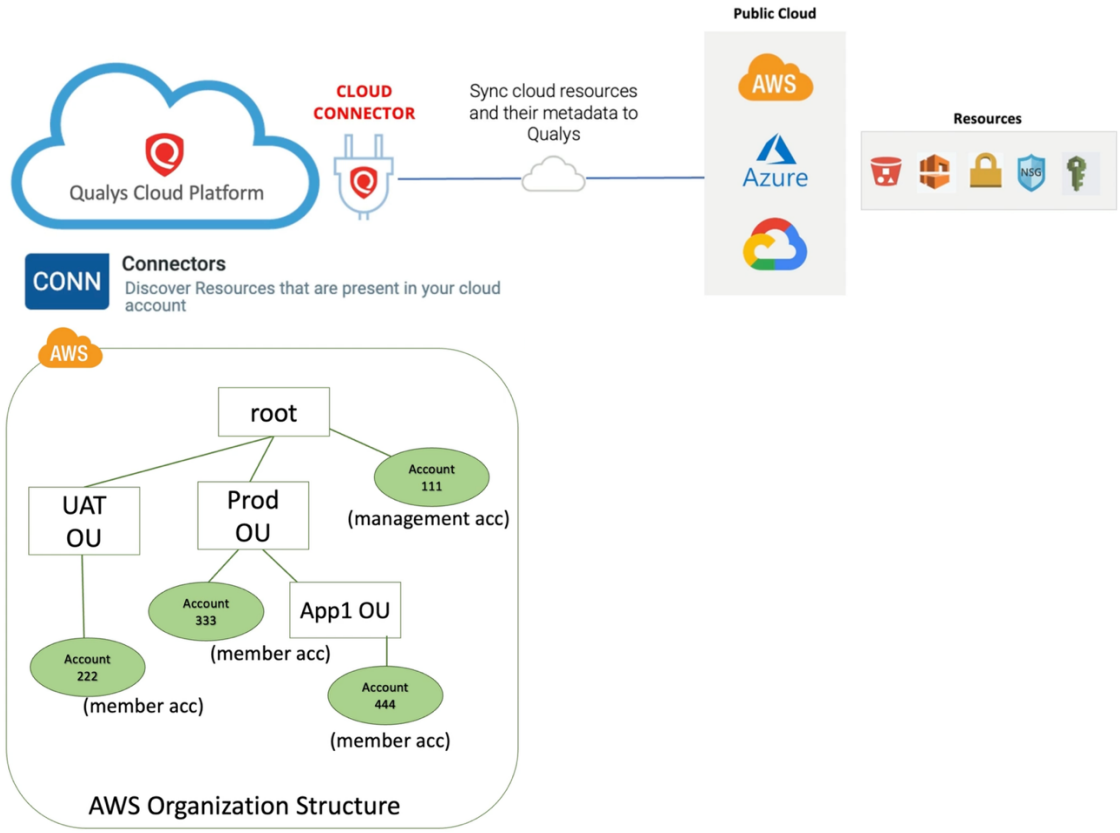


- **Cloud Connector** はクラウド上のリソースとメタデータを同期させます。
- **Cloud Agent** はクラウド上の VM にインストールし脆弱性情報を継続的に検出します。
- **仮想スキャナーアプライアンス**はクラウド上の VM にインストールし、プライベート仮想ネットワーク内のアセットをリモートスキャンします。
- **Container Sensor** は稼働中のコンテナやイメージレジストリの脆弱性、設定ミス、マルウェア、シークレット検出など検査します。
- **インターネットスキャナー**は、外部に公開しているアセットをリモートからスキャンし脆弱性を検出します。

セキュリティは常に可視性から始まります。クラウドコネクタは、すべてのクラウドリソースを一箇所で検出し、表示する機能を提供します。Qualys クラウドセキュリティは、さまざまなクラウドプラットフォーム向けのコネクタの導入

から始まります。クラウドネイティブのインフラストラクチャとアプリケーションのセキュリティを強化するために、Cloud Agents、Virtual Scanner Appliance、Container Sensor などの他の Qualys センサーの導入をご検討ください。Qualys クラウドプラットフォームに搭載された、すぐに使用できるインターネットスキャナは、クラウド境界のセキュリティギャップをスキャンする機能を提供します。

クラウドコネクター



- コネクタとは、Qualys がクラウドプロバイダーアカウントからリソースをポーリングできるようにする設定です。
- コネクタは、Qualys クラウドプラットフォームのコネクタアプリで設定および管理されます。
- 現在、Qualys は AWS、Microsoft Azure、Google Cloud Platform、OCI のコネクタをサポートしています。
- 組織コネクタを使用すると、多数のメンバーアカウントが存在する場合でも、コネクタの作成と管理のプロセスを簡素化できます。
- コネクタだけでなく、コネクタによって検出されたクラウドインスタンスや仮想マシンにもアセットタグを割り当てることができます。

- コネクタは、高速でゼロタッチの API ベーススキャンとスナップショットベーススキャンを使用して、クラウドワークロードをスキャンするように設定できます。

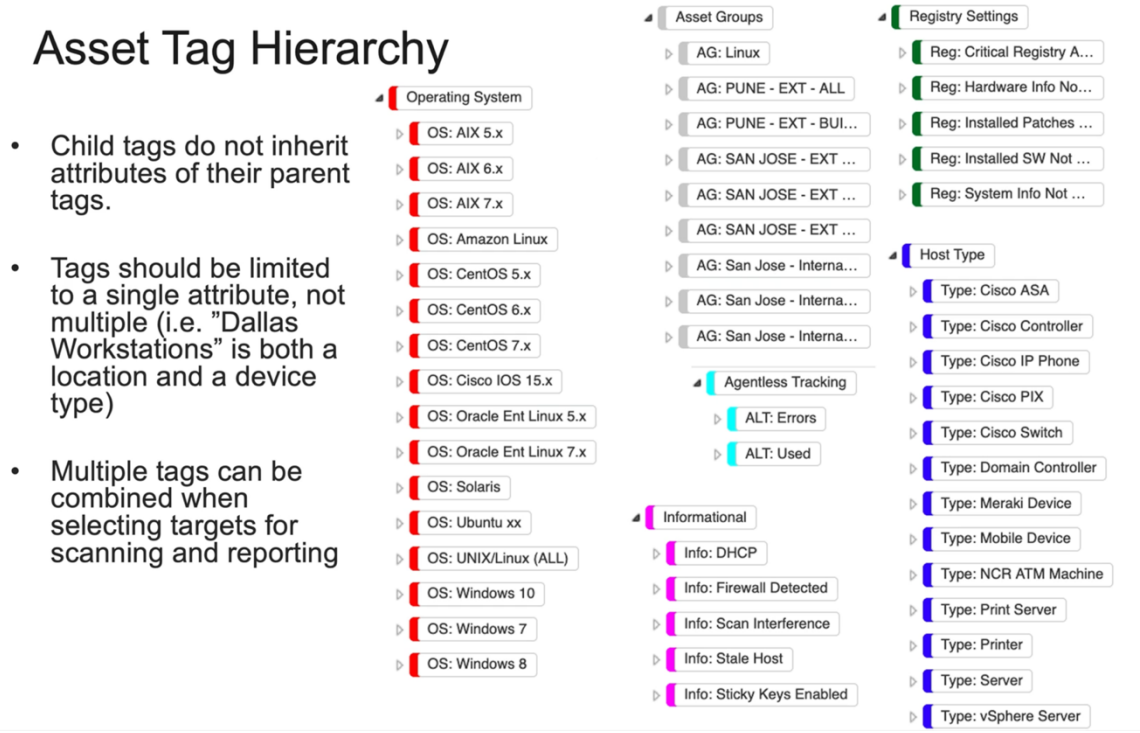
Asset Tag

アセットタグは、ホストをより柔軟かつスケーラブルに参照する方法を提供します。
アセットタグには、動的タグ(Dynamic tag)と静的タグ(Static tag)があります。
タグは階層構造になっています。親タグと子タグを持つことができます。

タグを最大限に活用する方法- この記事を参考にしてタグを設定してください。
この記事は、アセットの整理方法を理解しようとしているお客様にとって非常に役立ちます。
Qualys TruRisk を使用する場合は、タグにアセットの重要度を設定することが重要です。アルゴリズムの一部として、他の条件が同じであれば、重要度の高いアセットは TruRisk スコアが高くなります。

推奨事項

汎用アセットタグ（例：EC2）を少なくとも 1 つ作成し、コネクタによってインポートされたすべてのアセットに自動的にそのタグが適用されるようにすることをお勧めします。検出された EC2 メタデータに基づいて、EC2 アセットにさらにタグを追加できます。



実習：コネクター接続設定

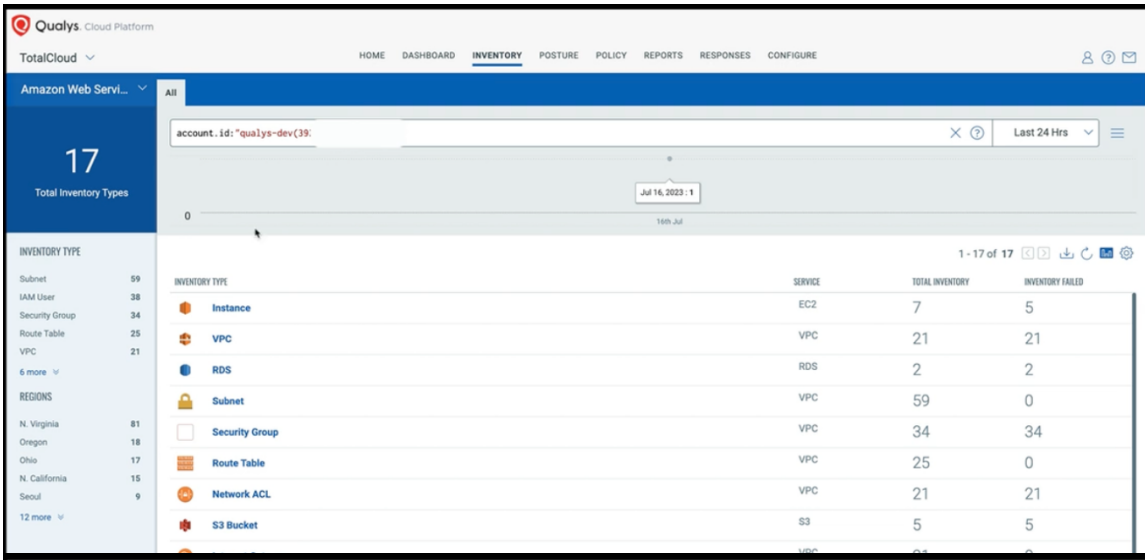
こちらの資料は各クラウドプロバイダーでのコネクター接続設定手順を案内していますので、ご参考としてください。

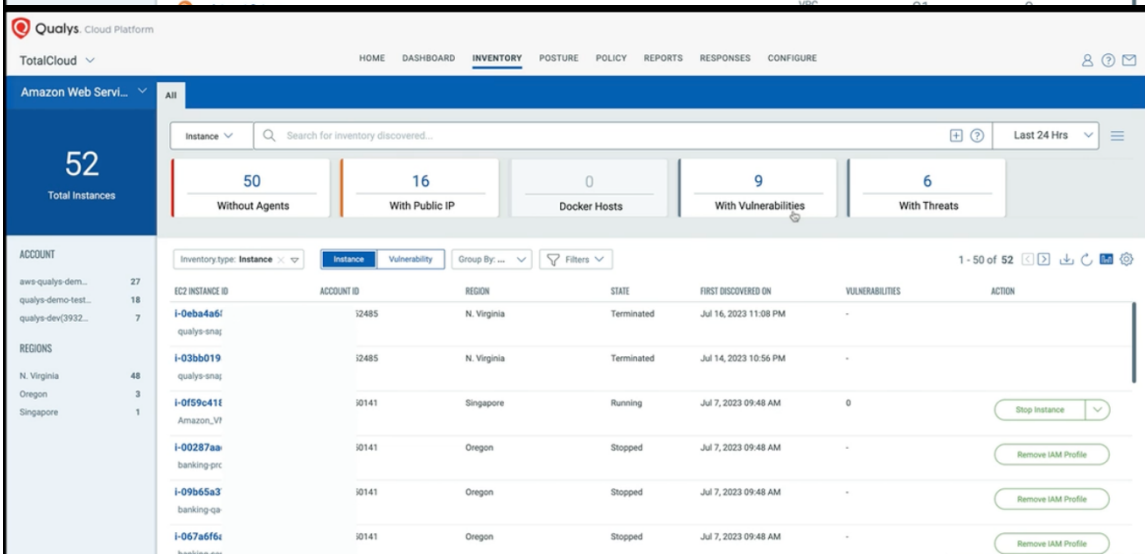
AWS Organization Connector

Azure Connector Deployment

GCP Organization Connector

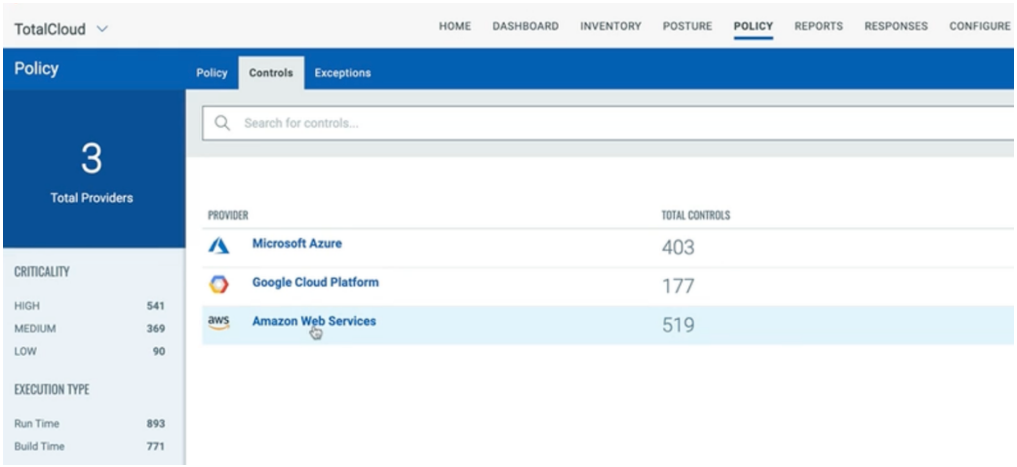
Cloud Inventory





- TotalCloud の「インベントリ」タブでは、クラウドインベントリの履歴とほぼリアルタイムのビューを表示できます。
- リソースタイプごとに、リソースの総数と、クラウドセキュリティ態勢評価に失敗したリソースが表示されます。
- クラウドリソース間の関係性を把握できます。
- フィルターとクエリを使用して、選択したタイプのリソースのみを表示できます。
- 時間フィルターを使用して事前定義された期間を選択するか、「特定の範囲」オプションを使用してカスタムの日付範囲を定義し、検索結果を絞り込むことができます。
- TotalCloud では、脆弱性の数は、以下のタイプのリソースに対してのみ表示されます。
- AWS: EC2 インスタンス、Azure: 仮想マシン、GCP: VM インスタンス
- 脆弱性データを取得するには、Qualys Scanner Appliance を使用したスキャン中にクラウドインスタンスまたは仮想マシンが検出されるか、Qualys Cloud Agent がインストールされている、またはコネクタ内で設定された API ベースまたはスナップショットベースのスキャン方法を使用してスキャンされている必要があります。

ポリシーとコントロール



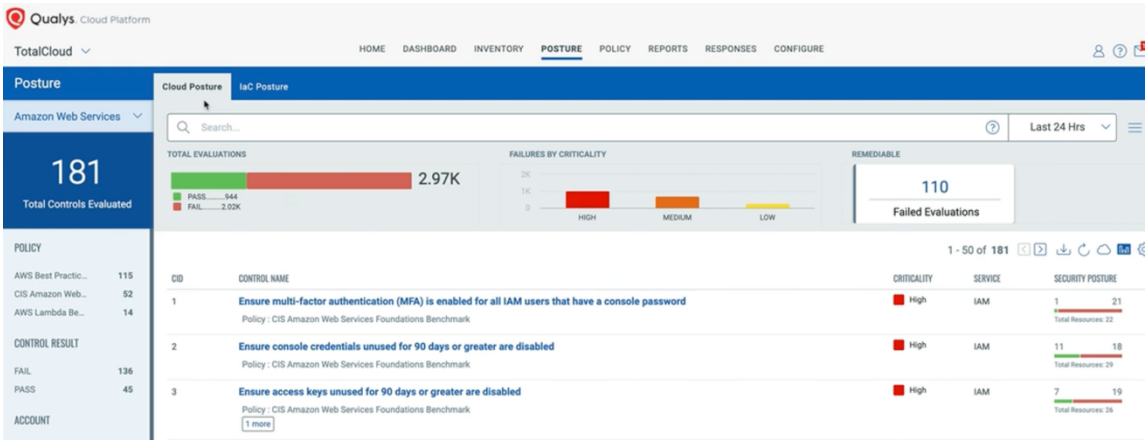
- コントロールは、一連のホストのコンプライアンスを測定および報告するために使用されるポリシーの構成要素です。
- 実行時コントロールとビルド時コントロールは、それぞれ環境に既にデプロイされているクラウドリソースと IaC テンプレート内に存在するクラウドリソースの評価に使用されます。
- ポリシーは、一連のリソースのコンプライアンスを測定および報告するために使用されるコントロールの集合です。
- Qualys が提供するすぐに使用可能なコントロールとポリシーをクラウドセキュリティ態勢の評価に使用することも、カスタム評価用に独自のコントロールとポリシーを作成することもできます。
- コントロール評価に失敗した場合に修復や緩和が不可能または現実的でないシナリオでは、例外処理が必要になる場合があります。

補助資料

Qualys TotalCloud Policy Control List

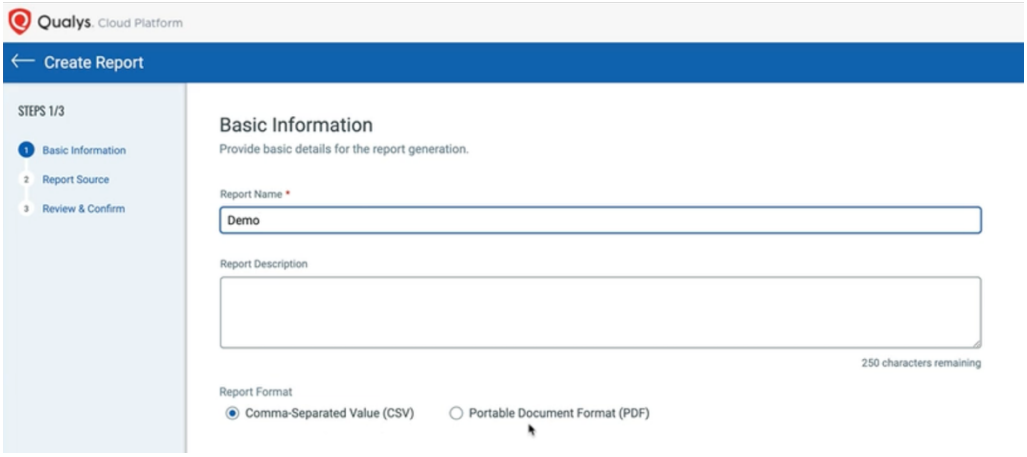
https://cdn2.qualys.com/docs/qualys_cloudview_policy_control_list.pdf

Cloud Security Posture



- TotalCloud の「ポスチャ」タブには、ランタイムコントロール（「クラウドポスチャ」サブタブ）とビルドタイムコントロール（「IaC ポスチャ」サブタブ）のコントロール評価結果が表示されます。
- クラウド資産全体の構成ミスを特定します。
- コントロールの不具合を修正する手順を表示します。
- 可視性の高い多くのコントロールに対して、ワンクリックで修正できます。

Cloud Security Posture Report



- クラウドリソースのコンプライアンス状況を確認するためのレポートを生成できます。
- クラウド環境内の複数のポリシーについて、リソースのコンプライアンス評価を確認するためのレポートを生成できます。
- Qualys クエリ言語 (QQL) のクエリ駆動型レポートウィザードを使用して、オンデマンドの評価レポートを生成できます。レポートが正常に作成されたら、クイックアクションメニューから CSV または PDF 形式でダウンロードすることもできます。
- 画面上のレポートでは、テンプレートを設定するための条件を設定し、対応するレポートを画面上で表示できます。
- レポートテンプレートで定義した条件に応じて、義務ベースのレポートとポリシーベースのレポートの 2 種類の画面上のレポートを生成できます。

実習

1. Qualys TotalCloud のインスタンスにログインします。
2. [ポリシー] > [コントロール] に移動し、AWS、Azure、GCP で使用可能なコントロールを確認します。
3. [ポリシー] > [ポリシー] に移動し、AWS、Azure、GCP で使用可能なポリシーを確認します。 [ホーム]に移動し脆弱性と設定ミスを発見します。 AWS/Azure/GCP コンプライアンスセキュリティ体制を確認します。
4. [レポート] > [レポート] に移動し、クラウド プロバイダーのベスト プラクティス ポリシーを選択して、AWS/Azure/GCP のレポートを作成します。
5. CSV または PDF レポートをダウンロードして確認します。

クラウドセキュリティポスチャレポート

Cloud Workload Scanning Methods

TotalCloud には、Qualys FlexScan による広範なスキャン機能が搭載されています。

- **API ベースのスキャン**は迅速な評価機能を提供しますが、包括的な脆弱性カバレッジは提供しません。
- **スナップショットベースの評価**では、AWS ワークロードのスナップショットイメージに対してスキャンを実行し、大量の脆弱性分析を行います。
- **エージェントベース**および**ネットワークベースのスキャン**（Scanner Appliance を使用）は、長時間実行されるワークロードに適しており、高精度で包括的な脆弱性カバレッジが求められる場合に適しています。

リソース

以下のクリックスルーチュートリアルでは、TotalCloud で利用可能な様々な方法を用いて評価を行うための手順を段階的に説明しています。

API ベースのスキャン
スナップショットベースのスキャン
クラウドペリメータースキャン

以下の Qualys ブログ記事では、スナップショットスキャンと他のスキャン方法を比較し、スナップショットスキャンがクラウドワークロードのスキャンに最適な方法ではない理由を説明しています。

ブログ：スナップショットスキャンだけでは不十分な理由

実習

1. Qualys TotalCloud インスタンスにログインします。
2. FlexScan オプション（API ベース、スナップショットベース、またはクラウドペリメータースキャン）のいずれかを使用して EC2 インスタンスをスキャンするように AWS コネクタを設定します。
3. スキャンが完了したら、「ホーム」>「脆弱性と設定ミスの検出」に移動します。

4. 脆弱性の総数とクラウドリスクスコアを確認します。

スキャンの基本

このビデオでは、Cloud Agent と Scanner Appliance のデータ収集方法の違いについて説明します。

1．Qualys は脆弱性評価のための様々なテクノロジーを提供し、ユーザーに柔軟なデータ収集方法を提供しています。
2．このアプライアンスは、ホストの脆弱性をリモートから把握できます。その有効性は、ホスト上のサービス/ポートの数と種類、個々のパケットに影響を与えるネットワークフィルタリングデバイスの有無などの要因によって異なります。
3．Qualys Cloud Agent は、各ホストにシステムサービスとしてローカルにインストールされ、ホストごとに 1 つのエージェントが存在します。システムレベルの権限で動作するこれらのエージェントは、スケジュールされた間隔で評価データを Qualys Cloud Platform に自動的に送信します。
4．包括的な脆弱性スキャンというビジネス要件に合わせて、Qualys Scanner Appliance と Cloud Agent の両方を同時に使用する組織もあります。

Cloud Agent

- 導入前に、ホスト OS が Cloud Agent（新しいタブで開きます）でサポートされていることを確認してください。
- Cloud Agent をホストシステムに導入する方法については、クリックスルー方式のステップバイステップのビデオをご覧ください。次のセクションで独自のエージェントを導入する際に役立ちます。
- 導入の主な手順の概要：1. アクティベーションキーを作成します。2. エージェントのインストールに使用するコマンドをコピーします。3. エージェントをダウンロードします。4. 構成プロファイルを構成します。5. ダウンロードしたエージェントを導入先のホストシステムに移動し、インストールコマンドを実行します。6. Cloud Agent インベントリにエージェントが表示されていることを確認します。
- ビデオではなくドキュメントをお探しの場合は、Cloud Agent スタートガイドをご覧ください。
- Cloud Agent のすべてのドキュメント - サポートされているすべてのオペレーティングシステム向けのエージェントのインストールガイドはこちらです。ご安心ください。導入準備ができたら、この資料を参考にしてください。
- エージェントを導入する主な方法は、コマンドライン、ゴールデンイメージ、ソフトウェア配布ツールの 3 つです。

- 必要に応じてプロキシ設定を考慮してください。
- エージェント接続のトラブルシューティング：このドキュメントでは、エージェント接続に関する問題のトラブルシューティング方法について説明します。
- Cloud Agent の詳細をさらに深く理解するには、Cloud Agent セルフペーストレーニングコースまたは講義ビデオライブラリ（をご覧ください。このシリーズの 2 番目のビデオはすでに視聴済みです。
- オンボーディングカードに記載されているすべてのリンクと推奨事項を確認してください。

実習

1．オンボーディングを完了するには、EC2 インスタンス、Azure 仮想マシン、GCP インスタンスに Qualys Cloud Agent のインスタンスにログインします。

2．「エージェント管理」>「アクティベーションキー」に移動し、「脆弱性管理」を選択した状態で新しいアクティベーションキーを作成します。

3．サポートされている OS プラットフォーム用のエージェントインストーラファイルとスクリプトをダウンロードします。

4．クラウドインスタンスに Cloud Agent をデプロイします。

5．Cloud Agent がサブスクリプションにレポートし、「エージェント管理」>「エージェント」タブに表示されていることを確認します。

オプション：Qualys Gateway Service

Qualys Gateway サービスは、エージェントデータを Qualys プラットフォームにプロキシするアプライアンスです。帯域幅を大幅に節約できるため、Qualys Patch Management をご利用の場合は非常に便利です。ご利用開始に必要なツールは以下をご覧ください。

1. AWS 上の Qualys ゲートウェイサーバ） - AWS 上の Cloud Agent のプロキシとして Qualys ゲートウェイサーバを使用している場合は、このガイドが設定に役立ちます。
2. Azure 上の Qualys ゲートウェイサーバ - Azure 上の Cloud Agent のプロキシとして Qualys ゲートウェイサーバを使用している場合は、このガイドが設定に役立ちます。
3. GCP VM 上の Qualys ゲートウェイサーバ- GCP 上の Cloud Agent のプロキシとして Qualys ゲートウェイサーバを使用している場合は、このガイドが設定に役立ちます。
4. ビデオシリーズ - このビデオシリーズでは、QGS の機能と正しい設定方法について説明しています。

Scanner Applicance

クラウドスキャナ - アカウントに既に関連付けられている Qualys クラウドスキャナを使用して外部からアセットをスキャンすると、外部からの脆弱性を「外部攻撃者の視点」で確認できます。つまり、Qualys でスキャナ以上のロールを持っている場合、外部（パブリック IP）アセットに対して自動的にスキャンを開始できます。

受信スキャントラフィックの IP 範囲：

1. VMDR 用の Qualys インスタンスにログインします。
2. [ヘルプ]（右上）> [バージョン情報] に移動します。
3. 受信スキャントラフィックを許可する必要がある IP 範囲を確認します。

Qualys スキャナアプライアンス - 内部（プライベート IP）アセットの場合は、Qualys スキャナアプライアンスを導入する必要があります。クラウドエージェントを導入していない場合は、Qualys スキャナアプライアンスを使用してすべてのホストと脆弱性をカバーします。スキャナはポイントアンドシュート方式で、スキャン中のみデータを収集します。スキャン後、収集された詳細情報はプラットフォームに送信されます。スキャナーのみを使用する場合、プラットフォーム内のデータは前回のスキャン時と同じ状態になります。最も徹底的かつ定期的に更新される脆弱性検出には、Cloud Agents と Qualys Scanner Appliance の使用をお勧めします。

一般的に、スキャナーはターゲットにできるだけ近い場所に導入するのが最適です。スキャナーがスキャン対象のターゲットへのルーティングと Qualys プラットフォームへのルーティングを確立し、ホームノードにコールインしてチェックインし、更新情報やスキャンジョブを受信できるようにする必要があります。

クラウドにおけるスキャナーアプライアンスの導入

Azure、AWS、GCE クラウド環境に Qualys Scanner Appliance を導入するための要件とプロセスを理解するには、以下のビデオをご覧ください。

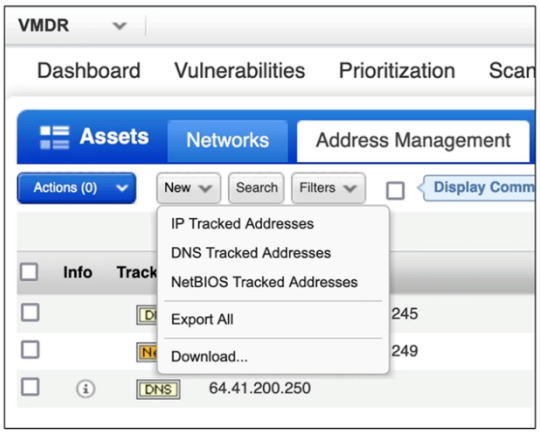
1 Azure での Scanner Appliance のデプロイ
2 AWS での Scanner Appliance のデプロイ
3 GCE での Scanner Appliance のデプロイ

その他の Scanner リソース

五感をフルに使って今この瞬間に向き合うとき、私たちは世界に喜びを招き入れます。過去の苦しみは過ぎ去り、未来はまだ開けていません。しかし、今この瞬間は、私たちの目を向けるのを待っている美しさに満ちています。

- サポートが必要な場合は、仮想スキャナーのデプロイガイドをご覧ください。このガイドでは、導入プロセスの概要と、サポートされている仮想化プラットフォームについて説明しています。
- スキャナーのトラブルシューティングに関するよくある質問をご紹介します。
- 仮想アプライアンスのサイズ設定- このリンクを使用して、仮想アプライアンスのサイズを適切に設定してください。

サブスクリプションへのスキャン・ターゲットの追加

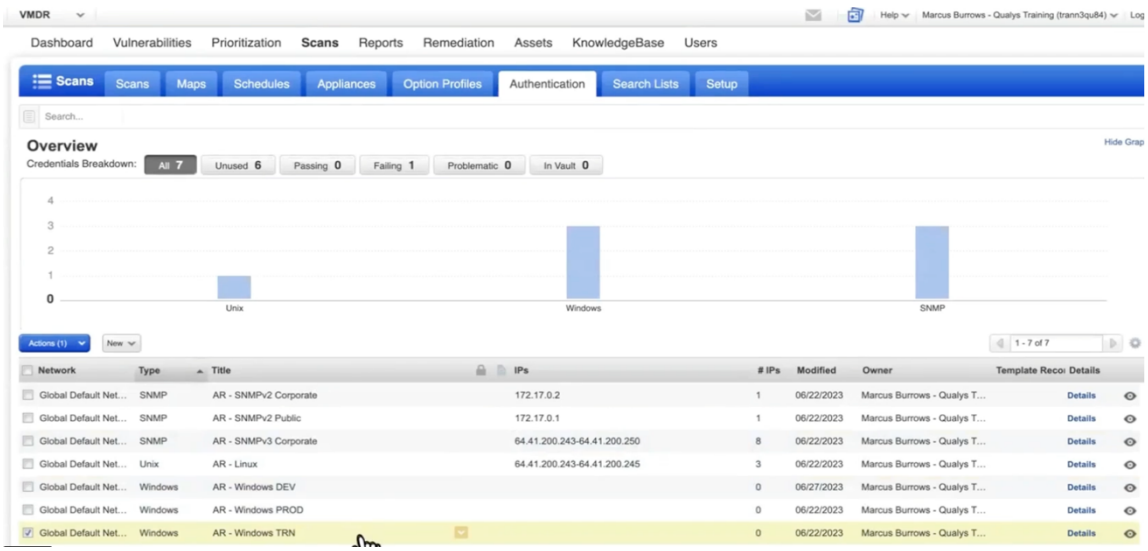


スキャナアプライアンスを使用してクラウドアセットをスキャンするには、これらのアセットを Qualys サブスクリプションに追加する必要があります。これは 1 回限りの設定です。

AWS および Azure コネクタは、EC2 インスタンスと Azure 仮想マシンをスキャン対象として Qualys サブスクリプションに自動的に追加するための特別なワークフローを提供します。

GCP またはその他のクラウド環境のクラウドインスタンスをスキャンするには、IP トラッキング、DNS トラッキング、NetBIOS トラッキングの 3 つのトラッキング方法から選択して、これらのアセットを VMDR サブスクリプションに追加する必要があります。

Scan Configuration



- 脆弱性評価スキャンを開始するには、少なくとも 1 つのスキャナアプライアンスが必要です。
- スキャンタスクのスキャナアプライアンスを選択するときは、スキャンのターゲットとするホスト資産を考慮する必要がありますが、これはスキャンを開始するために必要なもう一つのコンポーネントです。
- スキャンターゲットには、ネットブロックまたは特定の範囲の IP アドレス、または Qualys サブスクリプション内の 1 つの IP アドレスが含まれます。 ホスト IP をスキャンする前に、まずサブスクリプションに追加する必要があります。
- すべての脆弱性評価スキャンでは、さまざまなスキャン設定とスキャンオプションを含むオプションプロファイルを選択する必要があります。スキャンで認証が有効なオプション・プロファイルを使用する場合は、スキャン・ターゲットに対する認証に使用する認証レコードも作成する必要があります。

実習

オンボーディングを完了するには、仮想スキャナアプライアンスを自分でインストールしてスキャンを開始する必要があります。

1. Qualys VMDR のインスタンスにログインします。
2. [アプライアンス>スキャン] に移動し、AWS¥Azure¥GCE 環境に仮想スキャナアプライアンスをデプロイします。

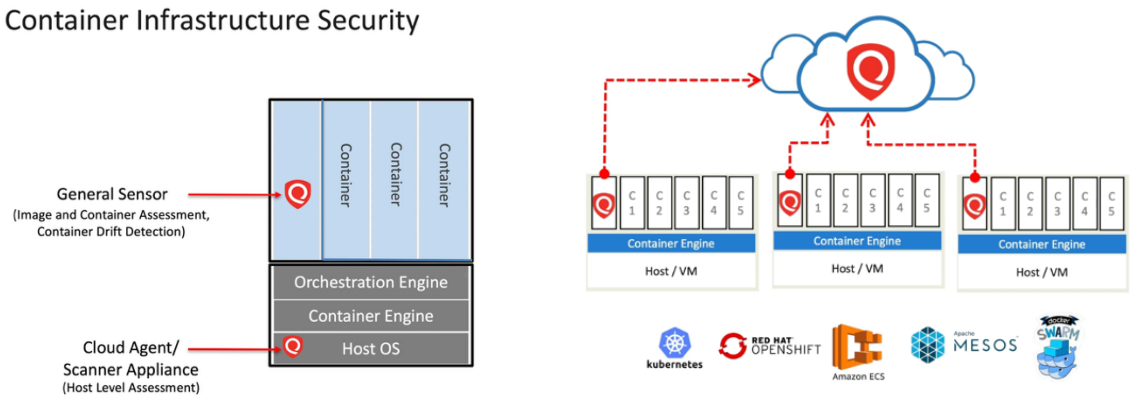
3. 検出された EC2 インスタンス/Azure 仮想マシンを VMDR アカウントに自動的に追加するか、GCP コンピューティング インスタンスを VMDR に追加するように AWS/Azure コネクタを構成します
4. [スキャン] > [スキャン] に移動し、クラウドインスタンスの認証されていないスキャン ¥ EC2 スキャンを起動します (これにより、スキャナーが正しく設定され、ネットワーク接続を確認するのに役立ちます)。

コンテナセキュリティ概 要

コンテナセキュリティの特徴

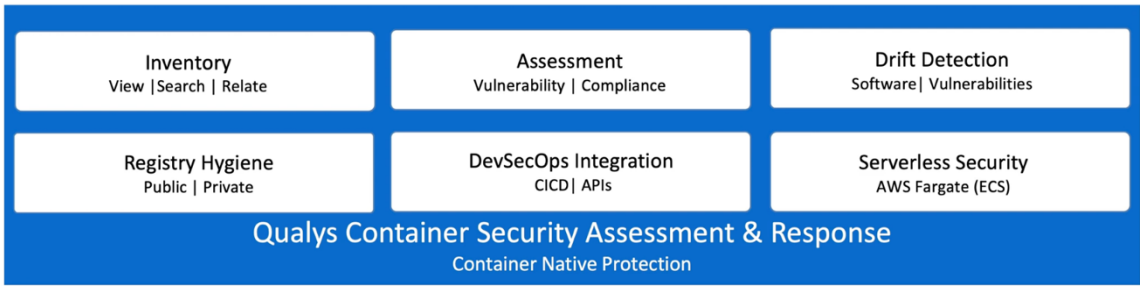
- コンテナ化されたアプリケーションをビルド、シップ、ランの各フェーズで保護
- Docker ホストにセンサーを導入し、イメージとコンテナのインベントリを取得
- 脆弱性管理と構成評価を実施

1. コンテナセンサーと導入先



- コンテナネイティブセンサーを Docker イメージとして提供。
- サポート環境：Docker、containerd、CRI-O、主要 Linux ディストリビューション。
- デプロイモード：一般センサー、レジストリセンサー、CI/CD センサー

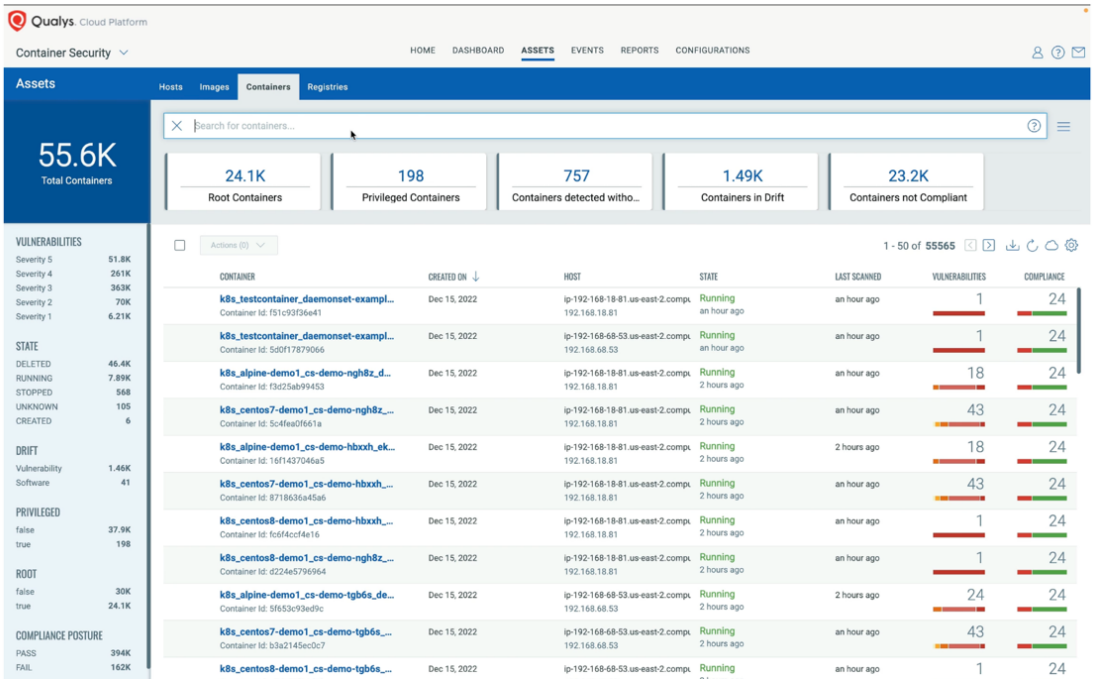
2．コンテナセキュリティ主な機能



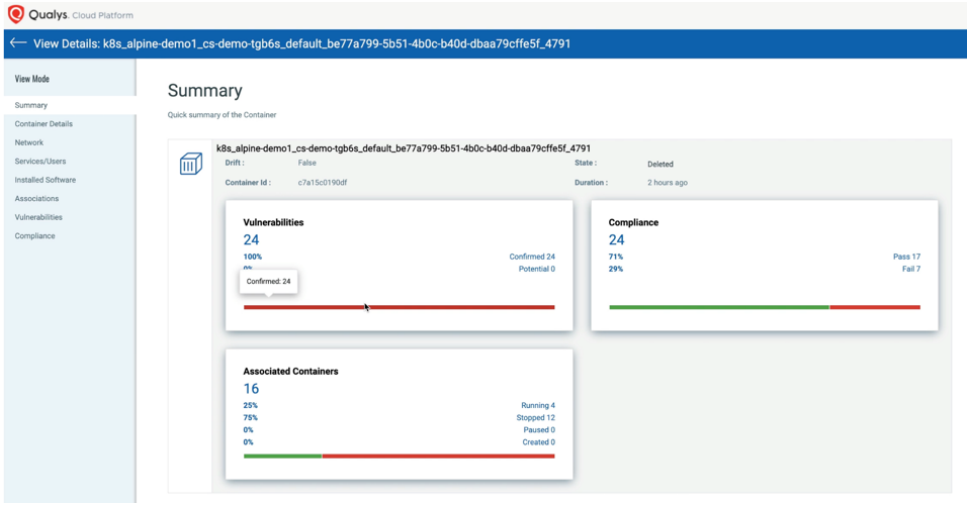
ドリフトコンテナの検出

- イメージから逸脱したコンテナ（追加ソフトウェアや脆弱性を含む）を特定
- ランタイム環境での不正変更を検出

3．コンテナー覧



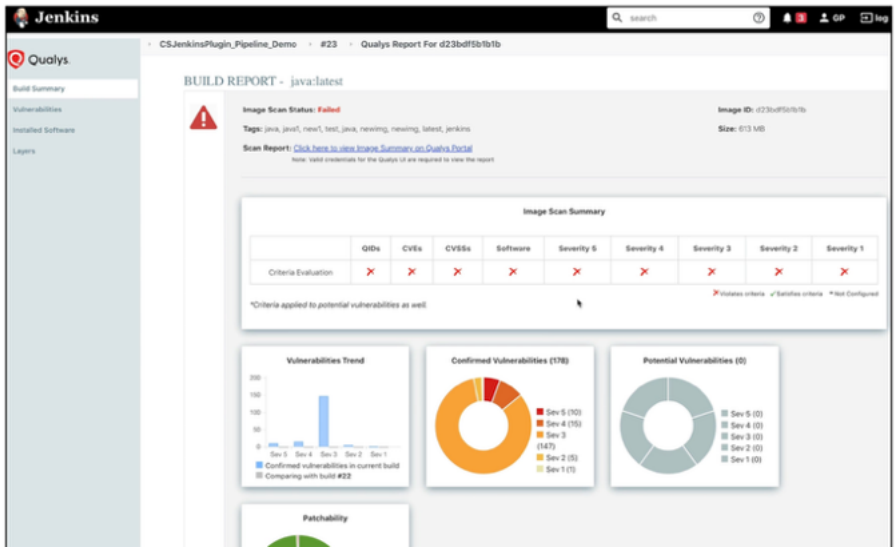
４．コンテナの詳細



５．CI/CD

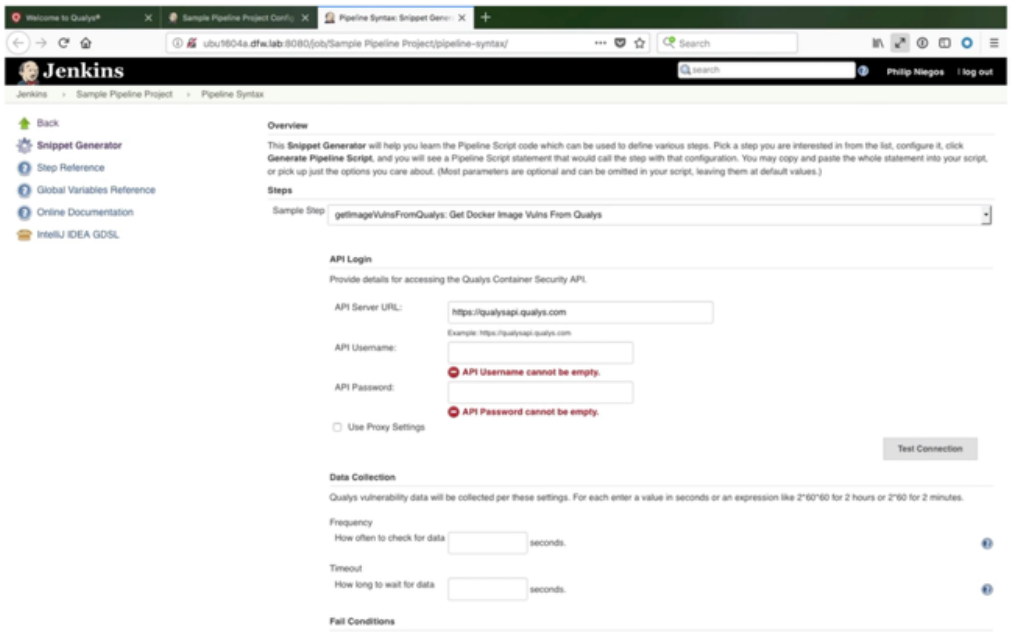
Qualys Container Security

Vulnerability Analysis Plug-in for Jenkins



レジストリスキャン

- 信頼できるイメージのみをレジストリに保持するため、レジストリスキャンを実施
- Jenkins や Bamboo などの CI/CD ツールと統合し、高リスクイメージを本番環境に入れない仕組みを提供



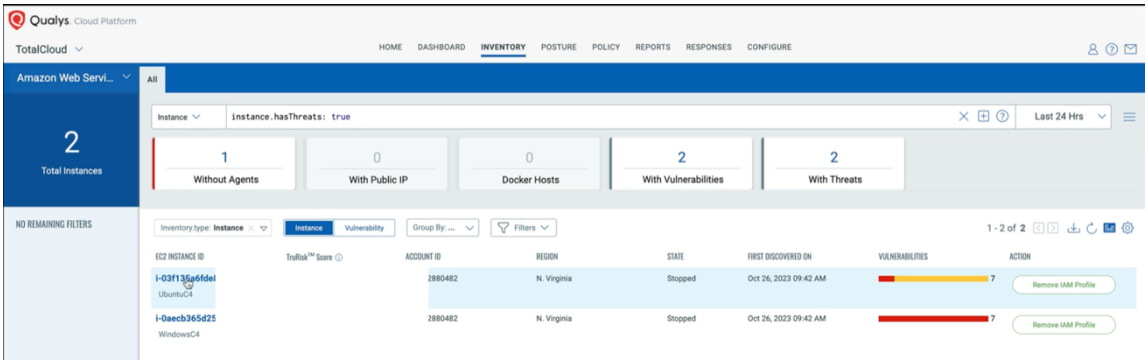
- Qualys Container Security (CS) は、コンテナライフサイクルの構築から展開まで、セキュリティを網羅します。
- イメージとコンテナを分析し、脆弱性や構成のギャップを検出し、リスクを特定します。
- 実行中のコンテナにおける脆弱性と構成の逸脱を検出します。
- HOWTO：コンテナセキュリティ：これらのクリックスルーチュートリアルでは、コンテナセンサーをさまざまな環境に展開する手順を解説し、Qualys Container Security のユースケースを理解できます。

Cloud Detection and Response

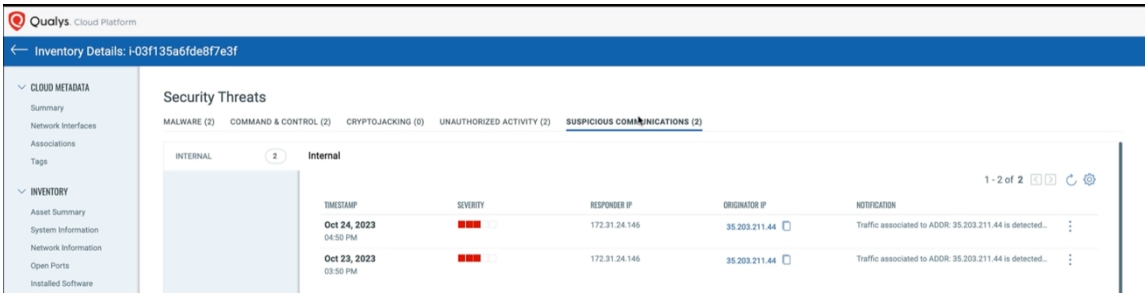
ランタイムセキュリティ

- クラウドネットワークトラフィックを検査し、不審な通信やアクティビティがないか確認します
- クラウドキルチェーンのさまざまなポイントで攻撃やゼロデイ脅威を検出します

- 積極的に調査されている資産を特定し、保護します
- 次のドキュメント CDR ユーザ ガイドでは、CDR の使用を開始するために必要な情報を提供します。



QQL: instance.hasThreats: true



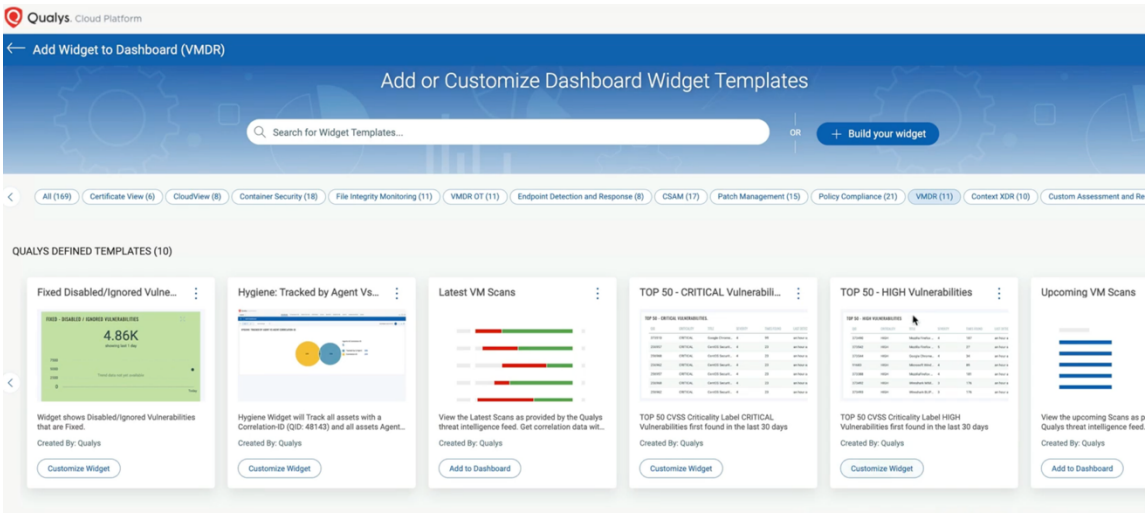
SUSPICIOU COMMUNICATIONS ではトラフィック上から怪しい通信を検出します。

レポート機能の紹介

成功のためのヒント

- Qualys での作業が目標と SLA に沿っていることを確認してください。
- 概要データにはダッシュボードを使用してください。
- QQL を使用してハンティングしてください。
- 詳細なレポートにはレポートテンプレートを使用してください。
- データハイジーン（データ衛生）を常に維持してください。
- レポートを実際に利用しているユーザーと話し合い、適切な量の情報が含まれていることを確認してください。

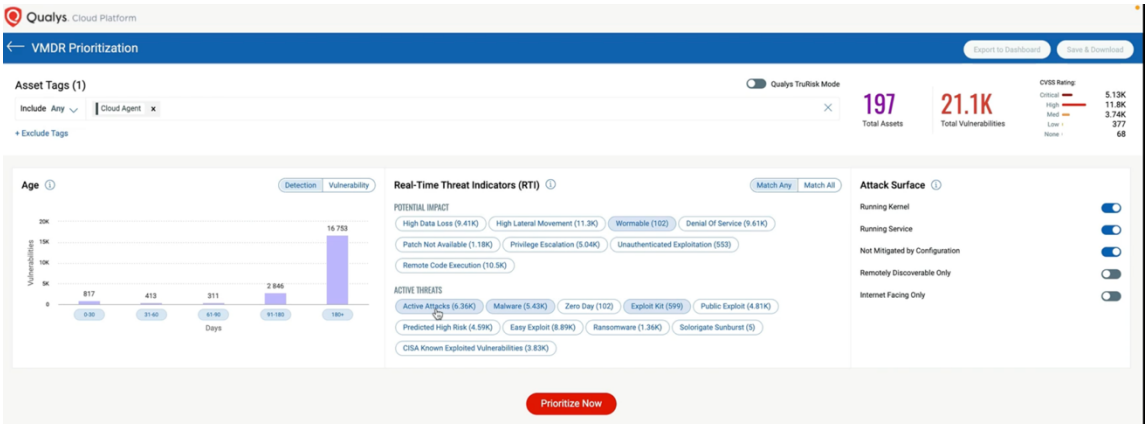
ダッシュボード



1. ダッシュボードは、データをすばやく可視化する場合に簡単に機能します。
2. 事前に構築されたダッシュボードとウィジェットをアカウントにインポートできます。
3. ダッシュボードから実用的なレポートにアクセスするには、2 回クリックするだけです。

参考資料：Unified Dashboards and Reporting Resources - Start Here

優先順位付け報告書



1. センサーを適切に展開し、適切なタグ付け構造を設定している場合、優先順位付けレポートは脆弱性管理プログラムにとって大きく簡単に成功します。 数回クリックするだけで、大きな重要なアクションを実行できます。
2. タグを使用してレポートを開始し、検出期間を使用してネットワークで脆弱性がいつ検出されたかを示すか、脆弱性の期間を使用して脆弱性が存在した期間を示します。
3. RTI は Qualys Threat Protection の一部です。 これにより、特定の脆弱性に脅威を追加するリスク要因に基づいて、さらに優先順位を付けることができます。
4. 攻撃対象領域では、最も影響の大きい脆弱性に優先順位を付けるためのフィルターも追加されます
5. 優先順位付けを TruRisk に設定すると、アルゴリズムを使用してさまざまな脆弱性リスクと脅威要因、および資産の重要度が考慮され、修復作業の優先順位付けに役立つ総合スコアが提供されます。

QQL

1. QL（Qualys Query Language）の位置づけ

- QL は Qualys クラウドプラットフォーム内でのレポート・分析ツール
- 従来の「バッチ処理で PDF やスプレッドシートを作成するレポートツール」とは異なり、インタラクティブな環境でデータを分析・可視化することを目的としている

2. 主な利用シナリオ

- **一時的な質問（One-off queries）**：
  - 例：特定の CVE に関する情報、影響を受ける資産数、特定ホストの状態など
  - レポートテンプレートを作成するより、クエリを直接実行する方が効率的
- **繰り返し発生する質問**：

- クエリを保存して再利用可能
- ダッシュボードウィジェットに組み込むことで、継続的に結果を表示・更新できる

3. ダッシュボードウィジェットの利点

- リアルタイム更新により、最新の情報を常に表示
- セキュリティトレンドの把握や、しきい値の達成をグラフィカルに確認可能
- テキストベースの QL よりも視覚的に優れた情報提供が可能

4. 従来型レポートも利用可能

- バッチレポートは、情報をキャプチャして運用チームに配布する際に有効
- ただし、今回の焦点はインタラクティブなクエリとダッシュボード構築

5. 前提条件

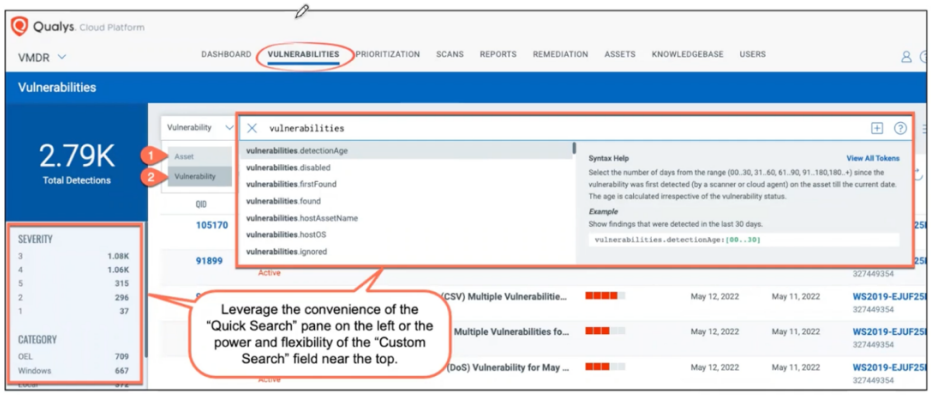
- Qualys ユーザーアカウントが必要
- ダッシュボード構築やウィジェット作成には、クエリ作成スキルが必須

Who Needs QQL?

Option	User Scope	Interactive	Batch	Vulnerability Details	Report Data Format
Dashboard Widgets	Qualys Users	X		High Level	Results exportable to PDF
On-demand QQL Queries	Qualys Users	X		High Level	Results exportable to CSV
VM Templates	Qualys & Non-Qualys Users		X	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
APIs (raw scan data)	Qualys Users		X	Detailed	CSV, JSON*
Hybrid – VM Templates & APIs	Qualys & Non-Qualys Users		X	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
Third Party Integration	Non-Qualys Users		X	High Level & Detailed	Varies depending on third party application

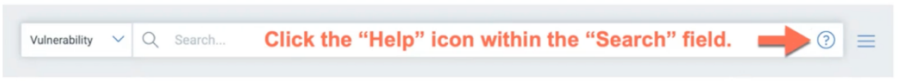
- QQL is ideal for Qualys users looking for a quick, interactive way to view asset and vulnerability findings and details.
- QQL is the foundation for building Dashboard Widgets.

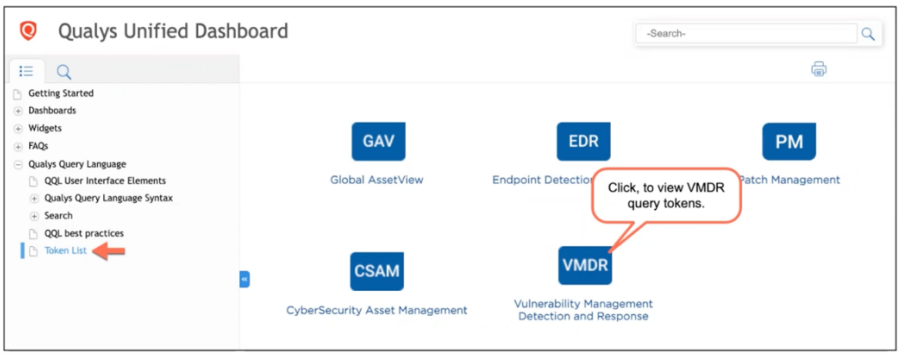
VMDR



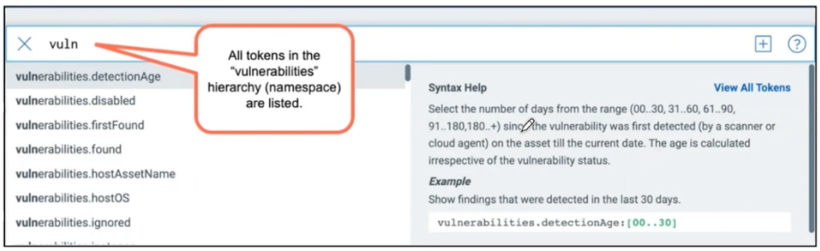
You will find a "Custom Search" field, along with a "Quick Search" pane, in the VULNERABILITIES section of VMDR.

VMDR Query Tokens





Token & Value Hints



vulnerabilities.vulnerability.title

Use quotes or backticks within values to help you find the title you're looking for.

Show findings for Microsoft vulnerabilities (unbroken character string):
`vulnerabilities.vulnerability.title:Microsoft`

Not Case Sensitive

Show findings for Microsoft Edge (character string with blank space):
`vulnerabilities.vulnerability.title:"Microsoft Edge"`

Not Case Sensitive

Show findings for Microsoft Edge Security Updates for April 2020:
`vulnerabilities.vulnerability.title:\`Microsoft Edge Security Update for April 2020\``

Case Sensitive

Integer & Number Range

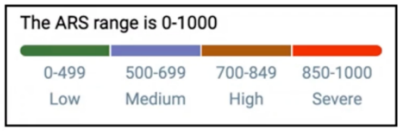
Use brackets or parenthesis, depending on your intended outcome.

- Greater than 850 and less than 1000:
  `(850 .. 1000)`
- Greater than or equal to 850 and less than or equal to 1000:
  `[850 .. 1000]`
- greater than 850 and less than or equal to 1000:
  `(850 .. 1000]`
- greater than or equal to 850 and less than 1000:
  `[850 .. 1000)`

greater than	**(**
less than	**)**
greater than or equal to	**[**
less than or equal to	**]**

Integer

VMDR 2.0
Asset
Risk
Score



riskScore

Use an integer value (0-1000) to help you find assets based on a specific risk score (ARS).

Show assets with a risk score equal to 800.
`riskScore:800`

Show assets with a Severe risk score (greater than 850)
`riskScore > 850`

Show assets with Medium or High scores
`riskScore:[500 .. 849]`

Integer Performance Tip

A specified list of integers provides better performance than an integer or number range containing only starting and ending values.

Use

```
vulnerabilities.severity: [1,2,3,4,5]
```

Rather than

```
vulnerabilities.severity: [1 .. 5]
```

Date & Date Range

vulnerabilities.vulnerability.published

Use a date range or specific date to specify when vulnerabilities were published in the KnowledgeBase.

Show vulnerabilities published on a specific date.

```
vulnerabilities.vulnerability.published:2022-07-19
```

yyyy-mm-dd

Show all vulnerabilities published before a specified date.

```
vulnerabilities.vulnerability.published < 2010-01-01
```

Show vulnerabilities published within calendar year 2021.

```
vulnerabilities.vulnerability.published:[2021-01-01 .. 2021-12-31]
```

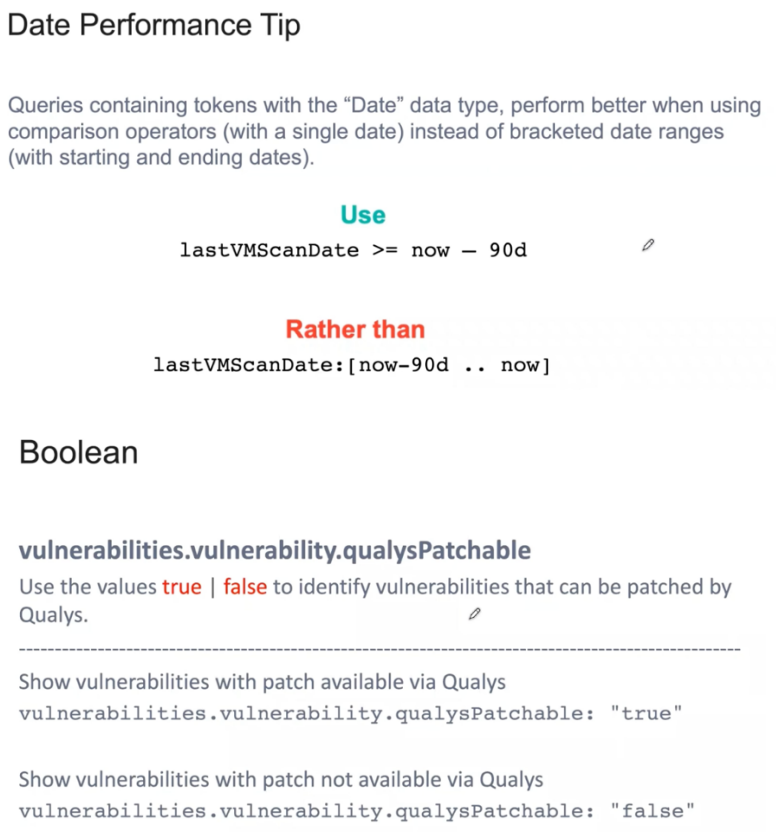
Show vulnerabilities published between Jan. 1, 2022, and now.

```
vulnerabilities.firstFound:[2022-01-01 .. now]
```

Time Units for use with “now”

y - year	now – 1y, now + 1y
M - month	now – 1M, now + 1M
w - week	now – 1w, now + 1w
d - day	now – 1d, now + 1d
h - hour	now – 1h, now + 1h
m - minute	now – 1m, now + 1m
s - second	now – 1s, now + 1s

For exclusive use with the “Date” and “Date Range” data types.



標準レポートテンプレート

1. 脆弱性レポート作成の前提条件

- レポートを作成するには、まず対象ホストの脆弱性評価が必要
- 評価方法：
    - スキャナーアプライアンスでスキャンする
    - Qualys Cloud Agent をインストールする

2. レポートテンプレートの選択

- Qualys コンソールの「Vulnerability Management」アプリケーション → 「Reports」セクション → 「Templates」タブでテンプレートを確認
- 利用可能なテンプレート：
    - **既存のプリセットテンプレート**（サブスクリプションに含まれる）

- **ライブラリからインポート**（「New」→「Import from library」で追加）
- **カスタムテンプレート作成**（「New」→テンプレートタイプ選択）

3. テンプレート設定の概要

- タイトルを設定
- 「Findings」タブで、以下の 2 種類のフィンドタイプを選択：
  - **Scan-based findings**（スキャン結果に基づくスナップショット）
  - **Host-based findings**（ホスト全体の最新状態を反映）

4. Scan-based findings の特徴

- スキャナーアプライアンスのみが生成（Cloud Agent は生成しない）
- 特徴：
  - 脆弱性ステータス（新規、アクティブ、修正済み、再オープン）は表示されない
  - トレンド情報は含まれない（スナップショットデータのため）
- 主な用途：
  - スキャン結果の分析
  - 認証失敗やスキャン時間のトラブルシューティング

5. Host-based findings の特徴

- スキャナーアプライアンスや Cloud Agent で収集した全スキャンデータを統合
- 特徴：
  - 脆弱性ステータスを追跡可能
  - トレンド情報を表示可能
  - 最新の資産状態を反映
- 注意点：
  - 認証モードの変更、スキャン対象ポート、ホストの生死状態に影響される
  - 資産追跡が正しく設定されていない場合、データの整合性に問題が出る

6. トレンド設定とレポートターゲット

- トレンド情報はデフォルトで過去 2 回分を表示
- カスタム期間設定可能（例：過去 1 か月）
- レポートターゲット：
  - 資産グループ、IP 範囲、タグで指定
  - 複数タグの「AND/OR」条件や除外設定も可能

7. Cloud Agent とスキャナーのデータ選択

- 両方のデータがある場合、以下を選択可能：
    - スキャンデータのみ
    - エージェントデータのみ
    - 両方。
- 選択内容は「Unified View」設定の有無に依存

スケジュールレポートの配 布

1. 配布グループの作成

- **目的**：レポートを非 Quality ユーザーに配布する
- **手順**：
    - ユーザーセクションの「Distribution Groups」タブで新しいグループを作成
    - タイトルを設定（例：「IT Admins」）
    - 非 Quality ユーザーのメールアドレスを追加（複数可、カンマ区切り）
    - 保存して完了

2. レポートのスケジューリング

- **手順**：
    - 「Reports」セクション → 「Schedules」タブ → 新規スケジュール作成
    - タイトル、テンプレート、フォーマット、対象を設定
    - スケジューリングを有効化し、日時・頻度を設定
        - 例：毎月最終金曜日に配布
    - 通知設定：
        - 送信元メールアドレスを指定
        - 宛先に先ほど作成した配布グループを追加
        - 件名・カスタムメッセージを設定
    - 配布方法：
        - デフォルトは「添付またはリンク」
        - 添付は 5MB 以下、超える場合はダウンロードリンク
        - 設定変更可能（添付のみ、リンクのみ、送信しない）

3. セキュリティ設定

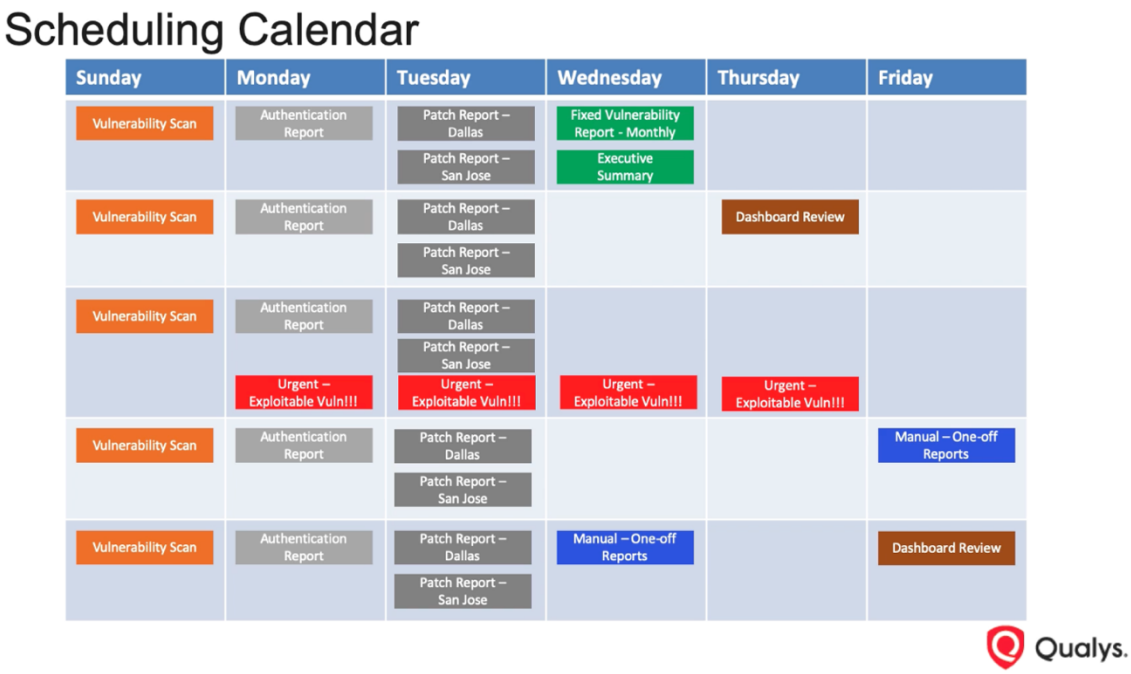
- **オプション**：
  - ダウンロード時のパスワード保護
  - ダウンロード回数の制限

4. ストレージ管理

- **デフォルト**：ユーザーごとに 200MB
- **最大**：500MB まで増加可能
- **追加機能**：暗号化 PDF のメール配布を有効化可能

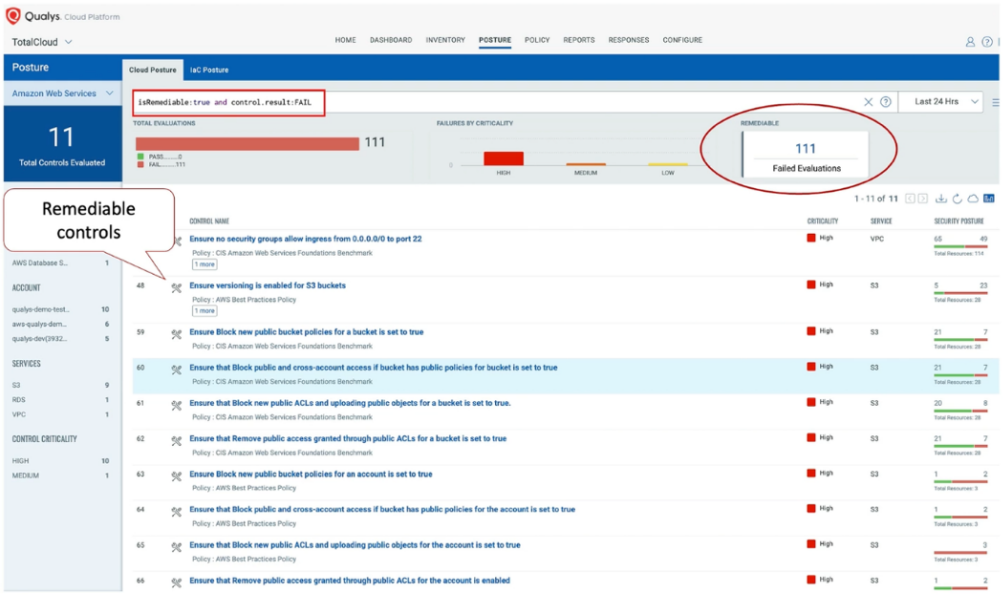
5. 脆弱性管理のスケジュール例

- **週次タスク**：
  - 週末：脆弱性スキャン
  - 月曜：認証レポート（認証失敗デバイスは再調査）
  - 火曜：パッチレポート → パッチチームへ
- **その他**：
  - 緊急脆弱性対応：毎日スキャン＆レポート
  - 月次レポート：修正済み脆弱性、エグゼクティブレポート
  - ダッシュボードで SLA 準拠状況を確認

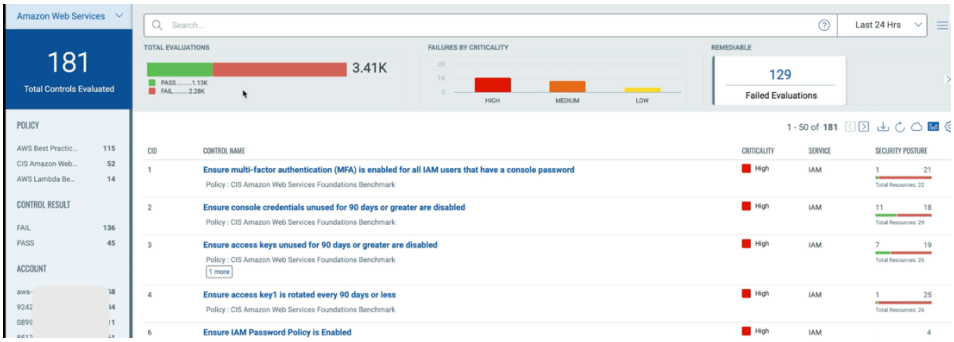


Remediation Misconfiguration

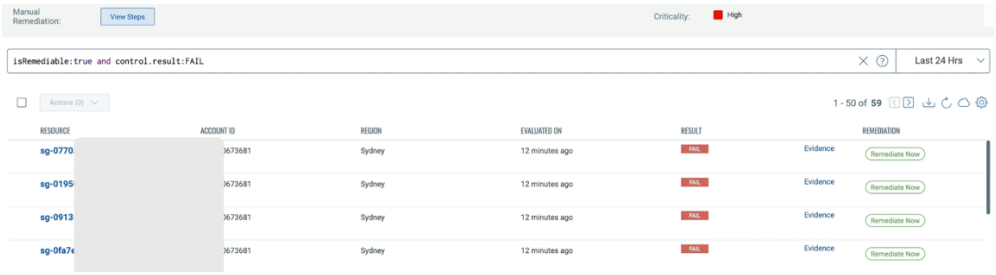
1. **リメディエーション機能の概要**
    - Total Cloud は、パブリッククラウド（AWS、Azure、GCP）のコントロール失敗を検出し、修正する機能を提供
    - 失敗したコントロールを特定し、ワンクリックで修正可能



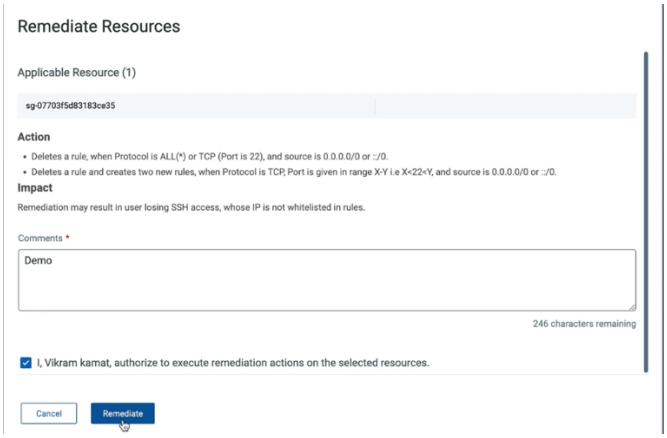
2. **ポスチャータブの役割**
    - コントロール評価結果（合格・不合格）を一覧表示
    - 「Remediable」カードには、修正可能な失敗リソースが表示される



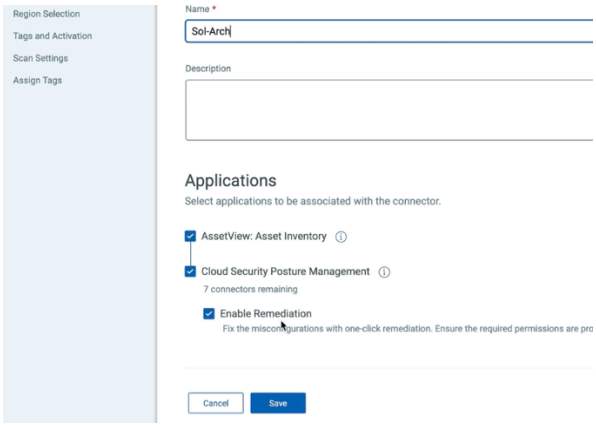
3. **具体例：セキュリティグループ評価**
    - ポート 22 へのアクセスを任意 IP に許可する設定は失敗と判定
    - ワンクリック修正で設定変更が可能



4. **修正実行の条件**
    - 修正には理由入力と認可選択が必要
    - Total Cloud が AWS に接続し、設定を変更する

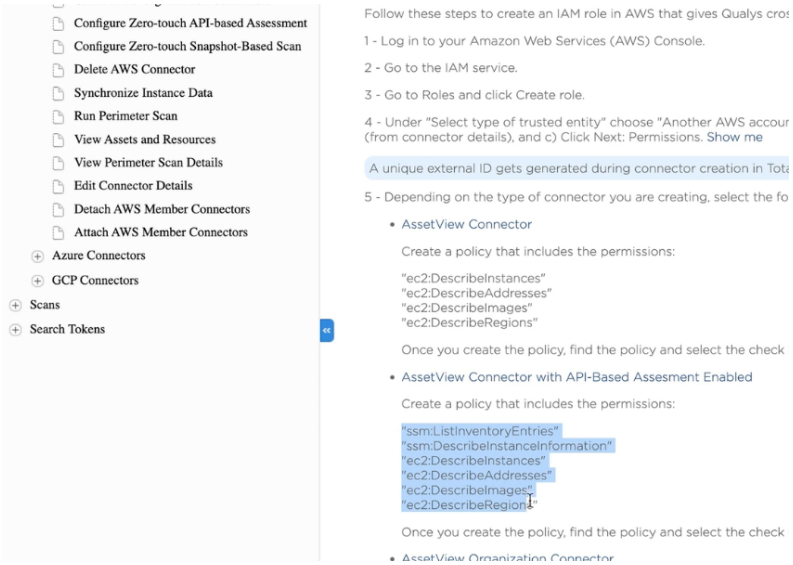


5. **コネクタ設定の重要性**
    - 修正機能を利用するには、対象クラウドアカウントのコネクタが「リメディエーション対応」に設定されていること
    - 必要な権限付与が必須。権限リストはオンラインヘルプで確認可能

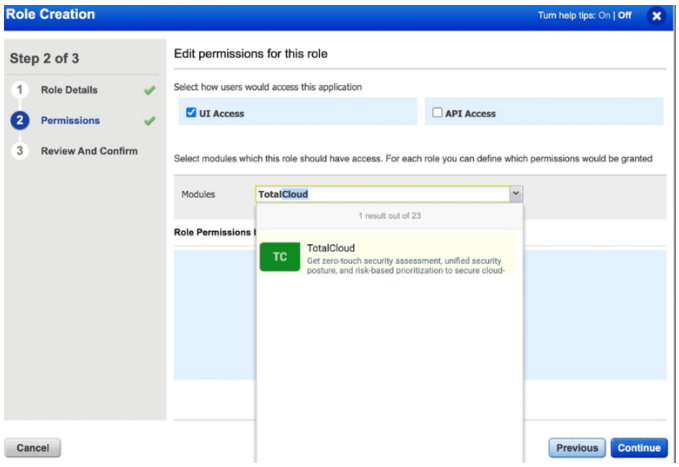


6. **権限の種類**
    - コネクタ構成（Asset View、API 評価、CSPM モジュールなど）に応じて必要な権限が異なる
    - Azure や GCP でも同様。

7. **追加機能：EC2 リソース操作**
    - 修正機能が有効な場合、EC2 インスタンスの停止や IAM プロファイル解除が可能



8. **ユーザー権限管理**
    - 修正操作には「Managed Remediation」権限が必要
    - 管理者または適切なロール設定が必須



オプションの脆弱性修正

1. Cloud Agent でのパッチ管理の有効化

- 最初に「Cloud Agent アプリケーション」で対象の資産を選択し、パッチ管理を有効化する
- 複数資産を一括で有効化する場合は、Actions ボタンを使用
- 有効化後、エージェントがパッチ情報を収集し、欠落パッチを検出する

2. Patch Management アプリケーションでの設定

- 次に「Patch Management アプリケーション」に移動し、Configuration セクションで資産を追加
- 「Licenses」でタグを追加（例：Cloud Agent タグ）
- Windows、Linux、Mac の OS を対象にパッチを展開可能になる

3. パッチジョブの作成

- 「Patches」セクションでパッチを選択し、新しいパッチジョブに追加
- ジョブ名は分かりやすい命名規則を使用
- 対象資産を選択（例：テスト環境→本番環境の順）
- スケジュール設定やオンデマンド実行が可能
- 再起動のタイミングやユーザーによる再起動延期の設定も可能

4. ジョブの実行とステータス確認

- ジョブ実行後、「Jobs」セクションで進捗を確認
- 成功・失敗の詳細やホストごとの情報を確認可能

5. 自動パッチ適用（ゼロタッチ）

- 「Prioritized Products」でアプリケーションファミリー別にパッチを確認
- Chrome や Firefox など、安定したパッチは自動適用ジョブを設定可能
- 毎週のスケジュールで最新パッチを自動展開することで、運用負荷を軽減

6. Patch Tuesday 対応

- テスト環境用と本番環境用の 2 つのパッチジョブを設定

- 本番ジョブはテストジョブを基に作成し、Patch Tuesday 後にスケジュール
- 問題が発生した場合は、本番ジョブを停止して再評価可能

7. VDR（脆弱性管理）との連携

- 「VMDR アプリケーション」で優先度の高い資産を選択し、脆弱性を確認
- 古い脆弱性を選択すると、必要な複数パッチを自動的に関連付けてパッチジョブを作成
- 脆弱性とパッチの関連付けは Qualys が自動で実施

Account Maintenance and Purging

1. ステール資産（Stale Assets）の定義

- ステール資産とは、終了済み・非アクティブ・廃止状態の資産を指します
- これらがレポートに残ると、以下の問題が発生します：
    - 存在しない脆弱性を追跡してしまう
    - セキュリティスコアや SLA 計算が歪む
    - パッチや修復レポートに不要な情報が含まれ、混乱を招く

2. パージの目的と概要

- **パージ＝ステール資産データを削除すること**
- 目的は、資産データを最新・正確・関連性のある状態に保つこと
- Qualys では、資産数やモジュールごとの内訳を確認できるダッシュボードを提供
- ダッシュボードのウィジェット例：
    - 6 か月以上更新されていない資産数
    - 脆弱性スキャンが 30 日・3 か月・6 か月行われていない資産数

3. 更新の定義

- 資産が「更新された」とみなされる条件：
    - スキャン実施

- クラウドコネクタの実行
- エージェントのチェックイン
- スキャナーアプライアンスによるスキャン

4. ベストプラクティス

- **注意点**：パージすると、そのホストのスキャンデータや検出情報は完全に削除され、復元不可
- 推奨事項：
  - パージ前に対象ホストのスキャンデータをエクスポート
  - 環境規模や IP 数を考慮（大量パージは時間がかかる）
  - 初回はパージ上限値を大きく設定し、バックログを処理後に調整

5. パージルールの設定方法

- **場所**：Qualys Cybersecurity Asset Management（CCM）モジュール
- 手順：
  1. 「ルール」→「資産パージルール」→「新規作成」
  2. 名前と説明を入力
  3. 資産選択条件：
     - クラウドエージェント基準
     - クラウドプロバイダメタデータ基準
     - 時間基準（他条件と組み合わせ）
- 例：
  - **クラウドエージェント資産**：90 日以上チェックインなし → パージ
    - 推奨：180 日以上更新なしは保持しない
  - **AWS 資産**：終了後 3 日以上 → パージ（推奨 14 日以内）
  - **Azure/GCP 資産**：終了後 3 日以上 → パージ

6. パージ制限と確認

- パージ上限値を設定（安全ロック）
- 実行後、ステータス確認：
  - 「Skipped」なら上限値を引き上げる
- サマリーで前回の一致資産数を確認し、余裕を持った上限値を設定

7. IP/DNS/NetBIOS 資産のパージ

- ネットワークスキャンで作成された資産は、パージルールでは削除不可。
- 削除方法：
    - VDR 資産検索で「最終スキャン日」フィルタを使用
    - 検索結果でチェックボックス選択 → 「パージ」または「すべてパージ」

Summary

スコープを理解する

Qualys を操作する前に、クラウド セキュリティ プログラムで実行しようとしていることの範囲を理解することが重要です。

セキュリティ ポリシーでは、評価対象の資産とその優先順位付け方法が示されていますか?

SLA とは何ですか?

こうした種類の質問は、セットアップを進めるのに役立ちます。

どのように優先順位をつけますか?

関連性と重要度に基づいて資産を分類することで、資産の整理を効率化します。

このステップにより、リソースの管理と保護に対する体系的なアプローチが確保されます。

資産を構造化することで、セキュリティ上の課題に対処し、リソースをより効率的に割り当てる能力が向上します。

資産運用管理

資産管理を使用すると、資産を整理できます。

タグとグループを使用するときは必ず命名規則に従ってください。

タグを使用して資産の重要度を設定してください。セキュリティポリシーでその重要度を規定する必要があります。資産の重要度は、重要度の高いホストに高い重み付けを割り当てるため、TruRisk にとって重要な要素です。

パージルールの設定

無駄のない関連性のあるデータセットを維持するために、データ消去に関する明確なルールを確立します。

効果的なパージルールは正確なレポート作成に貢献します。

データをいつどのように消去するかを定義することで、不要な混乱を減らすことができます。

レポート

強力なレポート メカニズムを実装して、セキュリティの状況を明確に把握できるようにします。

適切なレポート作成方法を確立することで、セキュリティ対策の有効性を理解し、情報に基づいた意思決定を促進できます。

主要な指標と関連データ ポイントに焦点を当てることで、情報過多を最小限に抑えます。

修復を自動化する

可能な場合は修復プロセスを自動化する機会を特定します。

自動化により、セキュリティの脅威への対応が効率化され、手動による介入が減り、応答時間が最小限に抑えられます。

自動修復を実装すると、全体的なセキュリティ戦略の効率と有効性が向上します。

リスクを軽減する

潜在的なセキュリティの脅威に対処するために、積極的なリスク軽減戦略を開発し、実装します。

リスクを評価して優先順位を付け、その影響を最小限に抑える対策を確立します。

明確に定義されたリスク軽減計画は、回復力のあるセキュリティ フレームワークに貢献し、新たな脅威からクラウド資産を保護するのに役立ちます。

以上