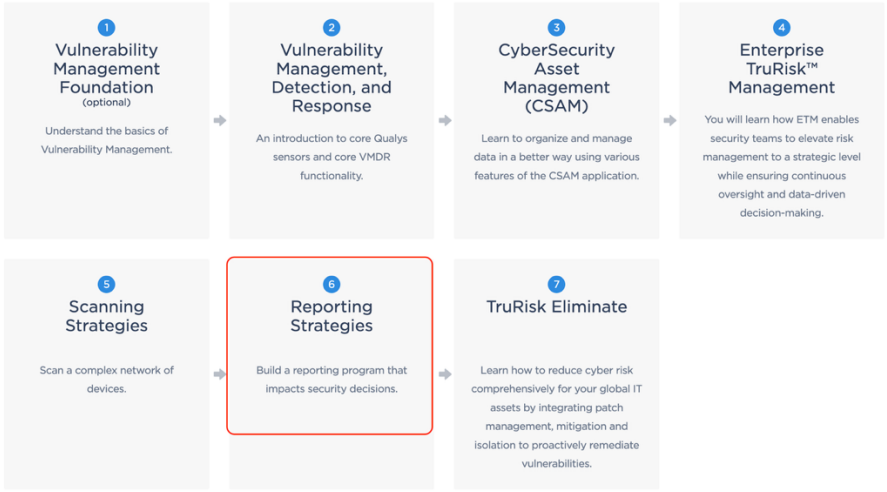
2025 年 10 月

Qualys レポート戦略とベストプラクティス 2.0

はじめに

このコースでは、環境内のデータ衛生を維持し、一貫性と信頼性の高いレポートを生成するためのベストプラクティスを学びます。また、組織内の様々なステークホルダー向けのレポートを生成するための、様々な戦略とツールの活用方法も学びます。

下記のフリートレニング⑥**Reporting Strategies** にエントリし、この資料とともにコースを完了する事を推奨します。
https://www.qualys.com/training/



データ収集の情報源

このレッスンでは、環境からデータを収集するために使用されるさまざまな Qualys センサーについて説明します。

Qualys センサー

Qualys にはデータを収集するさまざまなセンサーがあります。
データ収集に使用されるさまざまな Qualys センサーは次のとおりです。

- スキャナアプライアンス
- クラウドエージェント
- クラウドコネクタ
- コンテナセンサー
- パッシブセンサー
- 帯域外センサー(Out-of-band Sensor)

スキャナアプライアンス

オンプレミスまたはクラウド資産をスキャンするには、物理または仮想のイントラネット スキャナーと内部スキャナーが使用されます。

- 仮想またはハードウェア
- レガシーデータセンター
- 企業インフラ
- 継続的なセキュリティとコンプライアンスのスキャン

クラウドエージェント

クライアントとサーバーにインストールしてリアルタイムの可視性を実現できる軽量エージェント。動的 IP アドレスを持つ資産、リモートユーザーやローミングユーザー、一時的なクラウドインスタンス、外部スキャンの影響を受けやすいシステムに最適です。

- 軽量でマルチプラットフォーム
- オンプレミス、弾力性のあるクラウド、エンドポイント
- リアルタイムデータ収集
- セキュリティとコンプライアンスのための Qualys プラットフォームの継続的な評価

クラウドコネクタ

クラウド コネクタは、Amazon Web Services、Microsoft Azure、Google Cloud Platform などのクラウド プラットフォームからメタデータを収集します。

- API オーケストレーションによる完全自動化
- クラウド環境に展開されているすべてのインベントリを表示する

コンテナセンサー

コンテナ センサーは、Docker ベースのコンテナのイメージとして利用可能で、ビルドから実行までコンテナを検出、追跡し、継続的に保護するように設計されています。

パッシブセンサー

パッシブ センサーは物理アプライアンスまたは仮想アプライアンスとして利用可能で、すべてのネットワーク トラフィックを継続的に監視し、デバイスのプロファイルを作成し、資産のアクティビティにフラグを付けます。

- ネットワークをパッシブにスニッフィングする
- リアルタイムのデバイス検出と識別
- APT ネットワークトラフィックの識別
- ネットワークからマルウェアファイルを抽出する

帯域外センサー

帯域外構成評価は、切断された（エアギャップ）ネットワークに展開された資産の IT、構成、および脆弱性データを抽出するのに役立ちます。

可視性を高めるプラットフォームの構築

Qualys センサーは、インベントリ、脆弱性、脅威、コンプライアンス、クラウド、Web アプリケーションのデータをすべてプラットフォームに取り込みます。これにより、データを一箇所に集約できます。
ここからレポートに関する議論が始まります。レポートとは、Qualys プラットフォームで既に利用可能なデータを表示する様々な方法です。

レポート作成の考え方

このレッスンでは、Qualys 脆弱性管理アプリケーションでカスタムレポートを作成するために必要な基本的な概念とコンポーネントの概要を説明します。

一般的なベストプラクティス

レポートを設定するための一般的なベスト プラクティスを以下に示します。

1. Qualys レポートの設定が**組織のセキュリティ ポリシーと一致している**ことを確認してください。
2. **スケジュール設定** - レポートの頻度は**スキャンのルーチンに合わせてください。**例えば、毎週スキャンする場合は、毎週レポートを作成します。
3. 良好な傾向データを得るためには、**継続的なレポート作成を心がけてください。**頻繁に変更すると、データの測定が難しくなります。
4. **パージ** - パージを行わない場合は、データが古くなります。
5. 対象ユーザーとの関わりを維持します。**レポートの利用者と対話し、彼らが必要なものを入手していることを確認**します。
6. **集中的なホストベースのレポート**は、スキャンベースのレポートよりも**はるかに効率的**です。
7. **ダッシュボードを使用する** - **ダッシュボードはインタラクティブなレポート**なので、従来のレポートとダッシュボード スキーマの間でアプローチを変更する必要はありません。
8. **API** - レポート アーカイブ プログラムを実行するには **API を使用**します。

ポリシーと基準

Qualys は、連邦政府、医療、エネルギー、消費者向けパッケージングなど、多岐にわたる業種にサービスを提供しています。つまり、業種によって規制要件は異なります。**Qualys の重大度と検出タイプは独自のもの**であり、成熟したプログラムを導入していない企業を支援することを目的としています。
脆弱性のランク付けと優先順位付けには様々な方法があります。CVSS スコア、Qualys の深刻度レベル、リアルタイム脅威指標（RTI）などが挙げられます。**企業の深刻度ランク付けメカニズムは、これらの方法のいずれかに準拠する必要があります。**これにより、脆弱性への対処において、組織全体にわたる一貫したセキュリティポリシーを策定できます。その方法の一つとして、CVSS スコアの利用が挙げられます。

例えば、**CVSS スコアが 8.0 以上の場合、レベル 5（重大）に分類**されます。同様に、**レベル 4（高）、3（中）、2（低）、1（軽微）**は、以下の表に示すように、対応する CVSS スコアにマッピングされます。

企業の深刻度ランキング	CVSSv* スコア	企業脆弱性重大度評価基準
レベル 5（クリティカル）	**8.0～10.0**	この脆弱性により、次のことが可能になる場合があります。 • 攻撃者がリモート管理者またはルート権限を取得する • ホスト、アプリケーション、またはバックエンド データベースの公開（完全な読み取りおよび書き込みアクセス） • 攻撃者がリモートコマンドを発行したり任意のコードを実行したりできるようにする
レベル 4（高）	**6.0～7.9**	この脆弱性により、次のことが可能になる場合があります。 • 攻撃者はユーザー権限のみを乗っ取るか、完全なサービス拒否攻撃を実行します。 • たとえば、ホストファイルシステムやすべてのホストまたはアプリケーションユーザーのリストなどの部分的な公開（読み取りアクセスのみ）
レベル 3（中）	**4.0～5.9**	この脆弱性により、次のことが可能になる場合があります。 • 攻撃者がホストまたはアプリケーションを悪用または誤用したり、部分的なサービス拒否攻撃を実行したりすること • 攻撃者が追加の攻撃を調査できるようにする、機密性の高いホストまたはネットワークのセキュリティ構成の詳細またはソースコードへの部分的な露出（読み取りアクセスのみ）
レベル 2（低）	**2.0～3.9**	この脆弱性により、ソフトウェアの配布情報やバージョン情報などの情報が漏洩する可能性があります。攻撃者は、この情報を利用してホストやアプリケーションに対する潜在的な攻撃を調査する可能性があります。
レベル 1（最小）	**0.0～1.9**	この脆弱性により、ホストまたはアプリケーションに関する一般的な情報が公開される可能性があります。

あるいは、企業の重大度ランキングを **Qualys の重大度評価にマッピングすることもできます**。
たとえば、Qualys の重大度評価 4 と 5 は**高**、3 は**中**、1 と 2 は**低**に相当します。
特定された脆弱性は、1 から 5 までの重大度スケールに基づいてランク付けされます。

ランキングのオプション:

- CVSS ベーススコア（CVSS Base Scores）
- CVSS 一時スコア（CVSS Temporal Scores）
- Qualys 重大度ランキング（Qualys Severity Rankings）
- Qualys RTIs (Qualys Real Time Threat Indicators)

◉ Qualys は CVSS バージョン 2 と CVSS バージョン 3 をサポートしています 。CVSS スコアの詳細については、以下のリンクを参照してください。
https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/knowledgebase/cvss.htm

修復のための基準を設定する

組織は**修復を推進するための基準を設定する必要**があります。組織にとっての重大性と脅威は重要な役割を果たします。特定の種類の脆弱性に対する**修復の優先順位**は、最も高い攻撃対象領域と重大性に基づいて決定する必要があります。修復の優先順位付けを行う際には、資産の状況を考慮することも同様に重要です。例えば、重大度の高い脆弱性を持つ外部資産は、高い優先順位になります。レベル 5 は最高の重大度として使用されますが、これには脅威保護 RTI も含まれる場合があります。エンドポイントシステムも、「孤立している」可能性があるため、高い優先順位が付けられる場合があります。
修復のタイムラインは、以下の表に示すように、外部向け資産、内部向け資産、エンドポイント システムなどのインフラストラクチャ セグメントに基づいています。

企業の深刻度ランキング	外部向け資産	内部向け資産	エンドポイントシステム
レベル 5	1 日	30 日間	7 日間
レベル 4	7 日間	60 日間	30 日間
レベル 3	30 日間	次の生産リリース。90 日を超えないこと	90 日間
レベル 2 または 1	リスクに基づく意思決定	リスクに基づく意思決定	リスクに基づく意思決定

◉ 表に示されている SLA はあくまでも例示であり、実際の SLA は修復のためのリソースの可用性に基づいて組織ごとに異なる場合があります。

企業ポリシーと基準の整合

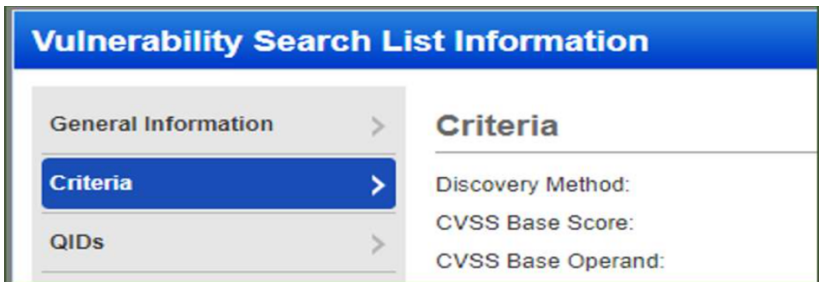
企業ポリシーを Qualys での取り組みと一致させたい場合、次のような疑問が生じることがあります。
質問: 企業の重大度ランキングに基づいて特定の脆弱性を選択するにはどうすればよいですか?
以下の表は、企業の深刻度ランキング、CVSSv* スコア、脆弱性の深刻度評価基準を示しています。

企業の深刻度ランキング	CVSSv* スコア	企業の脆弱性重大度評価基準
レベル 5（クリティカル）	8.0～10.0	この脆弱性により、次のことが可能になる場合があります。 • 攻撃者がリモート管理者またはルート権限を取得する • ホスト、アプリケーション、またはバックエンド データベースの公開（完全な読み取りおよび書き込みアクセス）
レベル 4（高）	6.0～7.9	この脆弱性により、次のことが可能になる場合があります。

企業の深刻度ランキング	CVSSv* スコア	企業の脆弱性重大度評価基準
		• 攻撃者はユーザー権限のみを乗っ取るか、完全なサービス拒否攻撃を実行します。
レベル 3（中）	**4.0～5.9**	この脆弱性により、次のことが可能になる場合があります。 • 攻撃者がホストまたはアプリケーションを悪用または誤用したり、部分的なサービス拒否攻撃を実行したりすること

Qualys 検索リスト と **検索クエリ**を使用すると、企業の重大度ランキングに基づいて特定の種類の脆弱性を選択できます。

上記の例では、脆弱性を深刻度と CVSS スコアでランク付けしているとします。環境に依存するため、外部脆弱性には基本スコア、内部脆弱性には時間的スコアを使用している可能性があります。そして、各資産について作成するレポートの種類（内部、外部、エンドポイント）に応じて、適切な検索リストを作成する必要があります。
脅威保護 RTI を使用してこれを実行することもできます。



計画 - ターゲットレポート

Qualys VM でレポートを計画する際には、まず組織のどの階層の担当者がレポートを確認し、どのような情報を確認する必要があるかを把握する必要があります。例えば、経営幹部はすべての Windows ワークステーションに必要な特定のパッチを確認する必要がありますか？それとも、全体的なリスク状況をより深く理解したいのでしょうか？
次に、事業分野について考えてみましょう。それぞれに個別のレポートを用意すべきでしょうか？
インフラストラクチャまたはネットワークセグメントは、クラウド資産とオンプレミス資産を分離するのに役立ちます。特定の資産に関連するリスクを把握するために、デバイスの種類ごとに資産を分離することができます。

セグメンテーション方法	例	説明
階層型レポート	C レベル、VP レベル、D レベル、マネージャー、技術 SME レベル。	レポートには組織の各レベルについてどのような技術的詳細を含める必要がありますか?

セグメンテーション方法	例	説明
組織内の事業部門	企業、子会社、部門、地域、支店。	社内の関係者向けにカスタマイズされたテンプレートを作成します。
インフラストラクチャまたは**ネットワークセグメント**	内部/外部/DMZ、オンプレミス/クラウド、本番環境、プレプロダクション環境、QA、テスト、開発、サンドボックス。	レポートを管理するチームと対処すべき優先順位に基づいてレポートを作成します。
技術チームまたは**修復チームの構造**	ハードウェア/ソフトウェア/帯域外、オペレーティング システム、アプリケーション、データベース、ネットワーク、サーバー、クライアント エンドポイント、ワイヤレス、内部/外部/DMZ、Web アプリケーション、アプライアンス、物理、仮想、ドメインなど。	レポートをデバイスの種類別に分類することで、より使いやすくなります。

レポートデータに影響を与える要因

はじめに

このレッスンでは、**レポートデータに影響を与え、分析や意思決定にレポートデータを使用する前に考慮する必要があるいくつかの要因について説明**します。

効果的なレポート作成の基盤としてのデータ品質

効果的なレポートは、脆弱性管理プログラムの成功に重要な役割を果たします。**データ品質**は、企業内の運用プロセスやトランザクションプロセス、そしてビジネス分析やレポートの信頼性にとって極めて重要です。
テクノロジーと運用上の前提条件は時間とともに変化します。その結果、IT インフラストラクチャも絶えず変化しています。これらの変化は、レポートデータにさまざまな影響を与えます。
したがって、レポート データの一貫性と信頼性に影響を与えるこれらの要因を理解し、データの健全性を維持するための適切なプロセスと標準を設定することが重要です。

レポートに影響を与える要因

以下のインタラクティブ **ビデオ**では、レポートに影響を与える要因について説明します。

Environment Factors that Impact Reports

Scan target configuration or environment specific factors:

- Change in host IP address or hostname
- Authentication failures
- Change in host "Live/Dead" Status
- Change in host OS
- Change in asset's business function
- Assets pending reboot following patching
- Ephemeral Cloud Instances

Ephemeral Cloud Instances

古くて一貫性のないデータの影響

適切なアセットハウスキーピングプロセスが導入されていない場合、アカウント内のデータが古くなり一貫性がなくなり、ダッシュボードやレポートに影響を及ぼします。
古くなった資産の脆弱性チケットはオープンのままとなり、リスク計算や SLA 指標に影響を及ぼします。また、修復のパフォーマンスにも影響を及ぼします。
さらに、古いアセットがサブスクリプション内に残っていて、新しい検出結果が入ったときに、関連付けられている IP アドレスまたはホスト名が別のアセットに割り当てられているとします。**これらの要因により、スキャン レポートに一貫性がなくなる可能性があります。**

- ダッシュボードとレポートが誤った結果を生成する
- 脆弱性チケットは引き続きオープンのままとなります
- 不正確なセキュリティリスク計算と SLA メトリック
- 不正確な修復パフォーマンス

導入

このレッスンでは、環境内でデータの健全性を維持し、一貫性と信頼性の高いレポートを生成するための推奨事項をいくつか示します。

データの一貫性の問題への対処

レポートデータに対して何らかのアクションを起こす前に、**レポートデータに影響を与える要因を評価**し、データハイジーンを維持するための適切な対策を講じることが重要です。**データハイジーンとは**、必要な時に適切な情報にアクセスできること、そして不要になった古いデータを保管しないことを保証するだけではありません。**データ管理に関するより効果的なプロセスを構築すること**です。

Addressing Data Consistency Issues

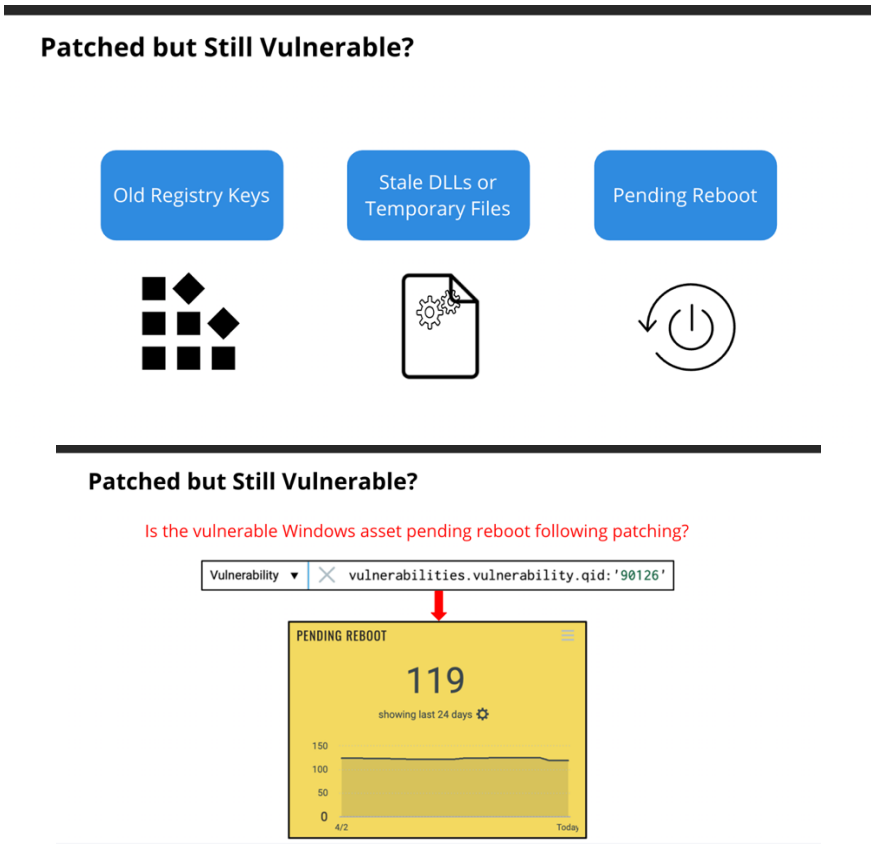
Scan Target Changes	Recommendations
• Authentication failures due to user credential changes • Assets pending reboot following patching • Change in the host “Live/Dead” Status • Change in host OS • Change in host IP address or hostname • Change in asset’s business function • Ephemeral Cloud Instances	• Use dashboards and authentication reports to identify and fix authentication issues quickly • Conduct regular assessment of your IT infrastructure to identify decommissioned and re-purposed assets • Configure asset housekeeping options in the scan optional profile settings • Setup rules to purge/remove impacted assets/agents to remove stale vulnerability data from your account

Addressing Data Consistency Issues

Scan Target Changes	Recommendations
• Changes in authentication mode • Changes to vulnerability detection criteria • Changes in target service ports	• Perform scans using a routine frequency • Simplify scanning by limiting the number of scan option profiles used for scanning • Implement appropriate user management to control who is allowed to make changes • Implement appropriate change management processes to prevent ad hoc changes to scan settings • Identify and purge impacted vulnerabilities following option profile changes when changes are necessary

パッチが適用されているがまだ脆弱がありますか?

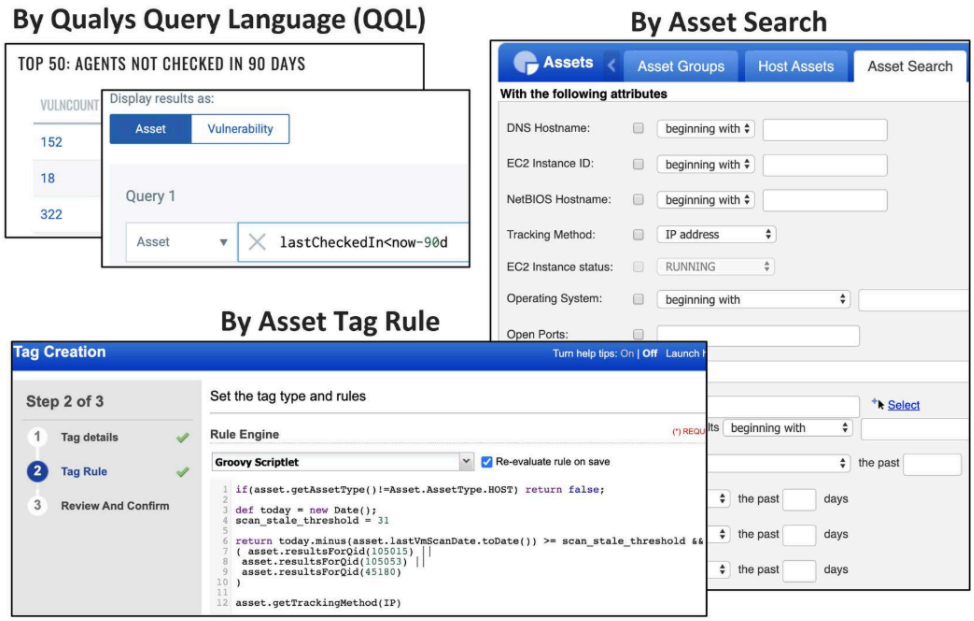
このトピックでは、脆弱性が依然としてフラグ付けされている理由を調査する方法を学習します。詳しは**トレーニングビデオ**をご参照下さい。



古い記録を特定する

古いレコードを識別するための基準はいくつか考えられます。**一般的な基準**としては、X 日間スキャンされていない資産、停止または終了状態の EC2 インスタンス、非アクティブな資産、または廃止された資産、認証に失敗したために脆弱性の検出結果が欠落したり矛盾したりしている資産などが挙げられます。
資産が識別され検証されたら、**UI または API 経由で消去**できます。

- VM/VMDR のアセット検索を使用して、パージ基準を満たすアセットを検索できます。
- QQL 検索クエリを使用して必要なアセットを検索したり、ダッシュボードウィジェットを作成してパージ対象のホストを特定したりすることもできます。QQL 検索クエリを使用してウィジェットを作成し、パージ対象のアセットを自動的に特定することもできます。
- 最後に、資産検索クエリ、脆弱性 QID、または Groovy スクリプトレットに基づく資産タグ ルールを使用して、削除する資産を自動的に識別してタグ付けすることもできます。
- エージェントレス追跡識別子と統合ビューが有効になっている場合も、古いレコードが発生する可能性があり、Qualys はリモート スキャン中に必要なエンティティ ID (ホスト ID、アセット ID など) を取得できません。
- これは通常、認証の失敗または資産に対する権限の問題が原因で発生します。



◉固有の追跡識別子とその使用例の詳細については、「スキャン戦略とベスト プラクティス」コースを参照してください。詳細については、次のドキュメントを参照してください。
https://success.qualys.com/discussions/s/article/000006149

パージルールの設定

トレーニングビデオでは、資産のデータを自動的に消去するための消去ルールを設定する方法について説明します。

パージ

資産の廃止は、技術的かつ管理的なプロセスです。IT インフラストラクチャを定期的に評価し、廃止または再利用する資産を特定し、それらの資産をパージしてアカウントから古い脆弱性データを削除する計画を立ててください。

1. パージとは、**古くなった資産データを削除すること**を指します。ホストを廃止する場合、または全く新しい役割（新しいオペレーティングシステム、新しいアプリケーション、新しい目的）で使用する場合、パージが必要になります。資産が頻繁に交換または削除される、非常に動的かつ一時的な環境では、パージが非常に重要になります。クラウドプロバイダー環境はその好例です。
2. 脆弱性管理アプリケーションで**ホストが消去**されると、インベントリ、脆弱性、および修復情報が削除されます。
3. ポリシー コンプライアンス アプリケーションで**ホストが消去**されると、コンプライアンスおよび例外履歴情報が削除されます。

◉パージ（何を、なぜ、いつ、どのように、データに何が起こるのか）の詳細については、以下のリンクをご覧ください。
https://success.qualys.com/discussions/s/article/000006221

IP を消去するか削除するか?

パージを行うと、サブスクリプション内の IP を保持し、サブスクリプションから関連データを削除できますが、IP を削除すると、IP と関連データがサブスクリプションから削除されます。
「パージ」または「IP の削除」オプションは、次のシナリオに基づいて使用できます。

- 資産が廃止され、その資産の IP アドレスが今後使用されることがない場合は、**REMOVE IP が推奨されるオプション**です。
- 資産が廃止され、IP アドレスが別の資産に転送される場合は、**PURGE オプションを使用して古いデータをすべて削除**します。

IP が別のアセットに再割り当てされた場合、または別の役割を担っている場合は、パージすることをお勧めします。
IP アドレスをスキャンしなくなり、その IP アドレスが再び使用されない場合は、削除することをお勧めします。実際には、同じ IP アドレスが再利用され、別のアセットに割り当てられる場合が多いため、IP アドレスを削除することはほとんどありません。そのため、ほとんどのシナリオでは IP アドレスをパージする方が適しています。こうすることで、廃止されたアセットの IP アドレスが新しいアセットに割り当てられた場合、スキャンのためにそのアセットを Qualys アカウントに再度追加する必要がなくなります。

資産のパージと削除の影響

ホストがパージされると、インベントリ、脆弱性、修復チケットの情報が削除されます。その他の情報はすべて保持されます。
ホストが削除されると、スケジュールされたスキャンとレポートは保持されますが、IP アドレスはグローバル除外リストに残ります。その他の情報はすべて削除されます。

影響を受けるエンティティ	パージ(Purge)	削除(REMOVE)
在庫情報	削除済み	削除済み
脆弱性履歴	削除済み	削除済み
修復チケット	削除済み	削除済み
コメント	変更なし	削除済み
ホストアセット	変更なし	削除済み
スキャン結果	変更なし	削除済み
資産グループ	変更なし	ホストがアセットグループから削除される
認証レコード	変更なし	認証レコードからホストが削除される
スケジュールスキャン/レポート	変更なし	スケジュールされたスキャン/レポートの対象リストからホストが削除される
グローバル除外リスト	変更なし	ホストがグローバル除外リストから削除される

パージする前に

パージを開始する前に、環境の規模とパージする IP アドレスの数を検討してください。多数の IP アドレスをパージすると時間がかかる場合があります。定期的にパージする必要がある場合は、API を使用して自動化することをお勧めします。

また、アセットをパージすると、そのアセットのすべてのホストスキャンデータ（検出結果）が Qualys アカウントから削除され、この操作は元に戻せませんのでご注意ください。そのため、パージする前に、該当するアセットのホストスキャンデータをエクスポートすることを検討してください。このデータのエクスポートには、Qualys API を使用することをお勧めします。API は一括データエクスポート操作に適しています。

レポートオプションについて

はじめに

このレッスンでは、脆弱性報告に使用されるオプションの概要を説明します。

レポートオプション

Qualys でデータを取得する方法は複数あります。**クエリ、ウィジェットとダッシュボード、VM レポート、API** などです。特定のオプションを選択する際には、Qualys ユーザーと非 Qualys ユーザーの両方がアクセスできるかどうか、インタラクティブ性、レポートに含めることができる詳細レベル、レポートのデータ形式などが考慮されることがあります。ここでは、ダッシュボード、QQL クエリ、VM テンプレートを使用したレポート作成について説明します。インタラクティブ レポートとバッチ レポートのオプションについては、以下で説明します。

インタラクティブレポート

オンデマンド QQL クエリとダッシュボードはインタラクティブであり、最も意味のある形式に到達するまでビューのフォーカスを再調整できます。

オプション	ユーザースコープ	脆弱性の詳細	レポートデータ形式
ダッシュボード	Qualys ユーザー	ハイレベル	PDF
オンデマンド QQL クエリ	Qualys ユーザー	ハイレベル	CSV

バッチレポート

API と VM テンプレートを使用して生成されたレポートは、これらのレポート オプションを使用して生成されたレポートからビューを再フォーカスできないため、非インタラクティブです。

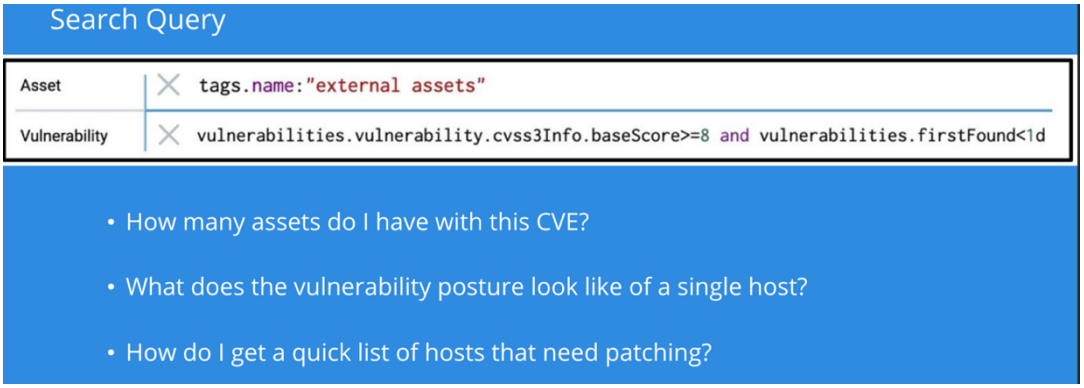
オプション	ユーザースコープ	脆弱性の詳細	レポートデータ形式
VM テンプレート	Qualys ユーザーと 非 Qualys ユーザー	高レベル＆詳細	CSV、DOCX、HTML、MHT、PDF、XML
API（生のスキャンデータ）	Qualys ユーザー	詳細	CSV、JSON*
ハイブリッド - VM テンプレートと API	Qualys ユーザーと 非 Qualys ユーザー	高レベル＆詳細	CSV、DOCX、HTML、MHT、PDF、XML

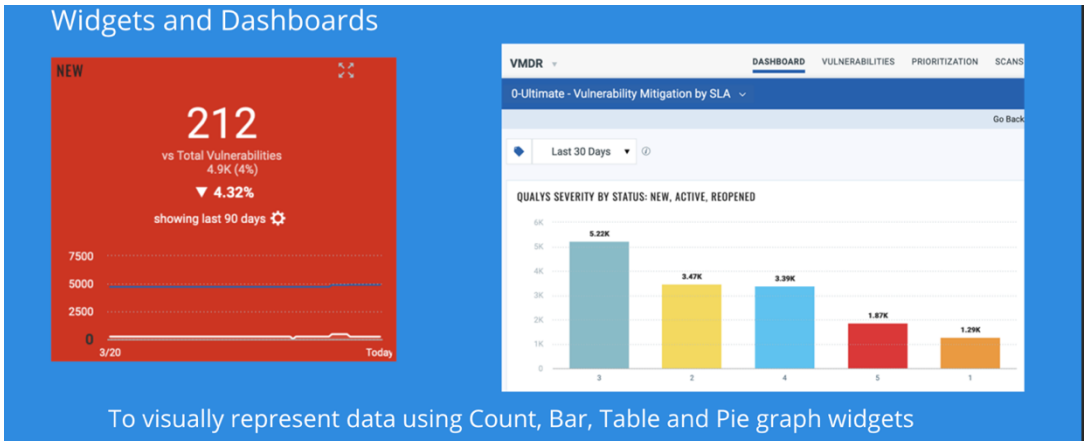
オプション	ユーザースコープ	脆弱性の詳細	レポートデータ形式
サードパーティ統合（QRADAR、Splunk、ServiceNow など）	Qualys 以外のユーザー	高レベル＆詳細	サードパーティのアプリケーションによって異なります

◉すべての API 抽出が JSON をサポートしているわけではありません。詳細については、API ガイドをご覧ください。

データはどこで入手すればよいですか?

トレーニングビデオでは、データを取得するために使用できるさまざまなオプションについて説明します。





レポート - ダッシュボード、ウィジェット、クエリ

はじめに

このレッスンでは、ダッシュボード、ウィジェット、脆弱性および資産追跡クエリなどのインタラクティブなレポートオプションを使用する際の考慮事項の概要を説明します。

インタラクティブレポートとバッチレポート

ダッシュボードとレポートデータの比較は、想像するほど単純ではありません。検出データの詳細な理解、適切なクエリフォーマット、適切なテンプレートまたは検索リストの選択が必要です。

考慮すべき点:

- すべてのダッシュボードが同じように作られているわけではない
- 履歴データを適切に処理するには、クエリで日付または時刻を指定してください。例：lastVmScanDate、lastPcScanDate、lastCheckedIn、firstFound、lastFound

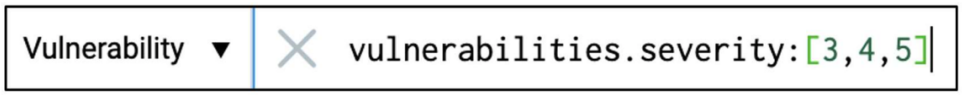
また、ダッシュボードのトレンドグラフは、監査に適した経時的なデータ追跡方法ではありません。データは不安定で、ウィジェットの変更で簡単に消去されてしまう可能性があるためです。これは、何かが変更されたことを視覚的に示し、ウィジェット数の大きな変化に気付くように設計されているだけです。このグラフがなければ、現状の数値しか把握できないため、カウントのコンテキストを提供するだけです。

ダッシュボード、ウィジェット、クエリ

ダッシュボード、ウィジェット、クエリを使用してデータを取得および視覚化できます。

クエリ

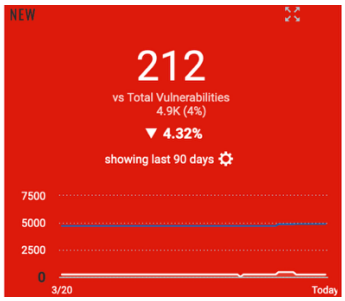
- データのリストを取得するためのコマンドが与えられます
- 質問への迅速な回答が必要な場合は、クエリを使用してください。例えば、特定のポートが開いているデバイスの数、SSL 脆弱性のあるデバイスの数、ゼロデイ脆弱性のあるデバイスの数などをクエリで簡単に調べることができます。



ウィジェット

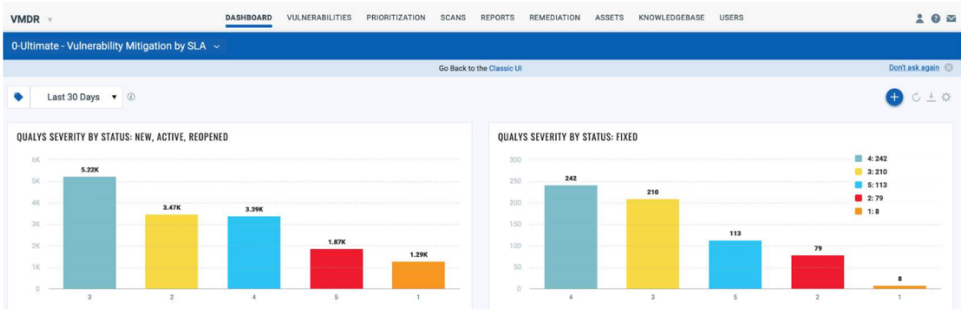
クエリを視覚的に表現したい場合は、ウィジェットを使用します。ウィジェットはダッシュボードにピン留めし、一定期間にわたって追跡できます。

- クエリの視覚的表現
- ダッシュボードの構成要素
- 傾向データを表示できます



ダッシュボード

- ダッシュボードは複数のウィジェットで構成されています
- 共通のテーマを持つウィジェットは、単一のダッシュボードに配置されます。例えば、SSL/TLS のダッシュボード、Cloud Agent の健全性に関するダッシュボード、Wanna Cry の脆弱性に関するダッシュボードなどです。



ダッシュボード、ウィジェット、クエリの場所

Qualys では、クエリ、ウィジェット、ダッシュボードを複数のアプリケーションで使用できます。どのアプリケーションを使用するかを知っておくことで、必要なデータを迅速に取得できます。

VM/VMDR ダッシュボード

- VM/VMDR ダッシュボードには、より強力で柔軟な検索オプションがあります。
- これは、検索クエリに一致する資産のリストと脆弱性のリストを提供するように設計されています。
- 新規、アクティブ、再開、修正済みの脆弱性が含まれます。
- 結果は資産と脆弱性として返されます。

脅威保護

- 脅威保護（TP）は AssetView の拡張機能として設計されています
- TP を使用して特定の脅威に一致する資産を検索する
- VMDR の脆弱性検索クエリでリアルタイム脅威指標（RTI）を使用することができます。
- VM サブスクリプションを持つアカウントで RTI 検索クエリトークンを使用するには、Threat Protection をサブスクリプションに追加する必要があります。詳細については、Qualys TAM にお問い合わせください。
- これは VMDR に含まれており、VMDR 優先順位付けレポートに RTI を提供します。これにより、発見された脆弱性の潜在的な影響や、既知または既存の脅威がある脆弱性を特定するのに役立ちます。

グローバルアセットビュー（GAV）/サイバーセキュリティ資産管理（CSAM）

- Global AssetView（GAV）/CyberSecurity Asset Management（CSAM）を使用すると、資産のより詳細な情報を得ることができます。
- これには、AssetView で収集された標準的な資産データに加えて、メーカー名、製品名、ソフトウェアバージョン、ハードウェア、ソフトウェア製品のリリース日、サポート終了日、ライセンスカテゴリなどの詳細が含まれます。
- ハードウェア、ソフトウェア、OS などの正規化および分類された資産メタデータ
- 結果はアセットとして返されます。

ダッシュボードの使い方

ダッシュボードは以下を使用して作成できます。

- Qualys が提供する既存のウィジェットテンプレート
- 既存のウィジェットをカスタマイズするか、
- ニーズに合わせたウィジェットの作成

テンプレートを使用したダッシュボードの作成

- Qualys は、ダッシュボードのリストにすぐに追加して資産の監視を開始できる、すぐに使用できるダッシュボードテンプレートを提供します。
- テンプレートの中から、資産のデータ入力ニーズに合ったものを選択し、ダッシュボードを作成してください。ダッシュボードはすぐに使用できます。
- ダッシュボードにウィジェットを追加したり、既存のウィジェットを編集したり、ウィジェットのレイアウトを変更したり、ダッシュボードでさまざまな操作を行うことができます。
- 新しいテンプレートは、公開されるとすぐに Qualys アカウントのテンプレート ライブラリに定期的に追加されます。

Qualys コミュニティからのダッシュボードとウィジェットのインポート

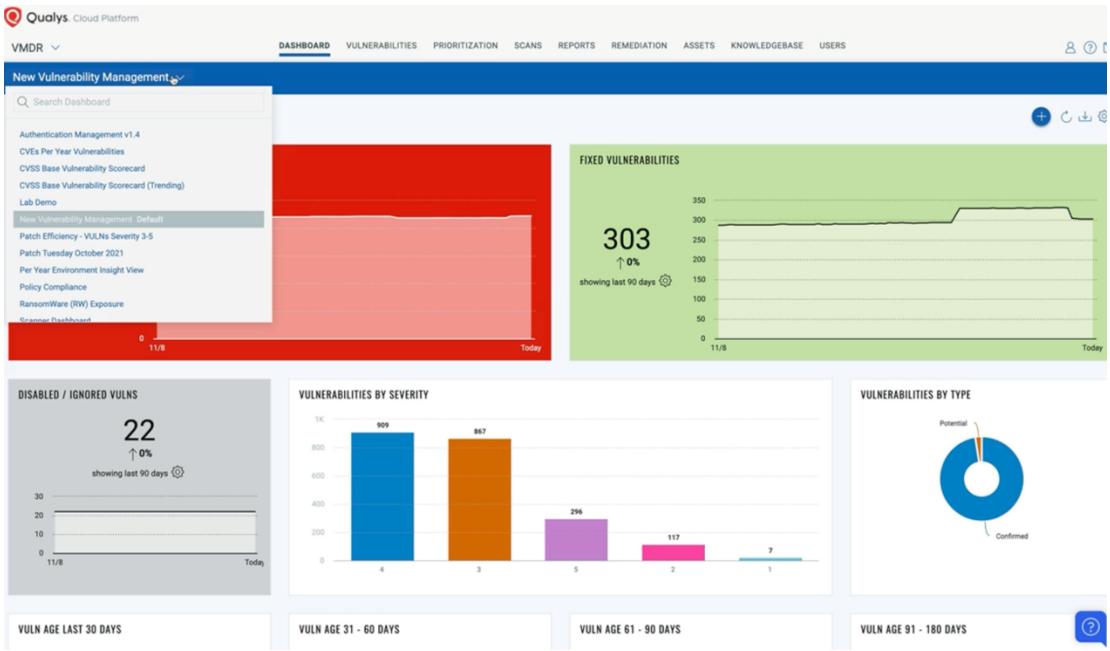
- ダッシュボード構築用のテンプレートを使用するだけでなく、Qualys コミュニティで利用可能なダッシュボードを Qualys アカウントにインポートすることもできます。
- すぐにインポートできる VM/VMDR ダッシュボードへのリンクは、次の場所にあります: https://success.qualys.com/discussions/s/article/000005975（新しいタブで開きます）
- https://success.qualys.com/discussions/s/article/000006212 を参照してください。（新しいタブで開きます）ダッシュボードの JSON ファイルを Qualys アカウントにインポートする方法の詳細については、

ダッシュボードをゼロから作成する

- これは検索クエリを使用して独自のウィジェットを作成する必要があるため、最も手間がかかります。
- このアプローチを使用して独自のカスタムダッシュボードとウィジェットを構築するには、クエリトークンとクエリフォーマットの要件とベストプラクティスを十分に理解することが前提条件です。

ダッシュボードナビゲーション

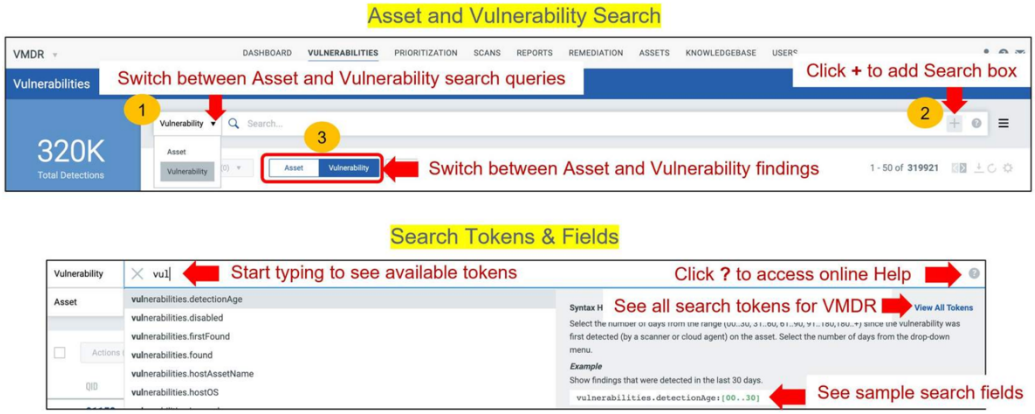
トレーニングビデオは、ダッシュボードに含まれる機能を理解するのに役立ちます。



VM/VMDR 検索

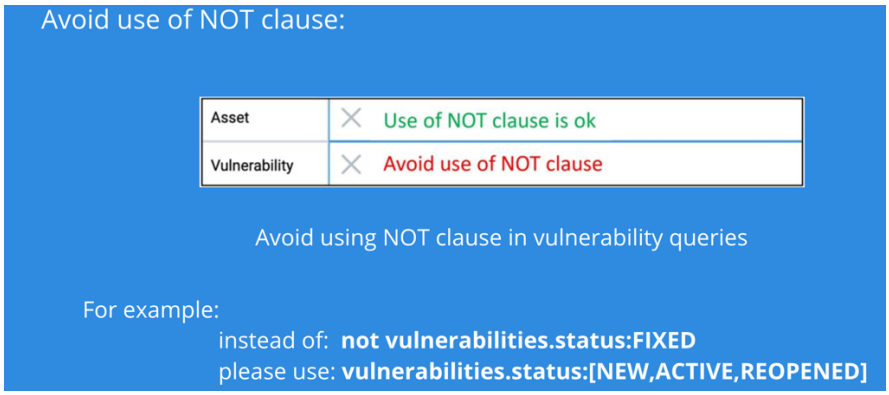
VM/VMDR 検索の「脆弱性」セクションでは、統合された増分検索とブラウジング エクスペリエンスが提供され、資産に関するすべての情報を検索できます。

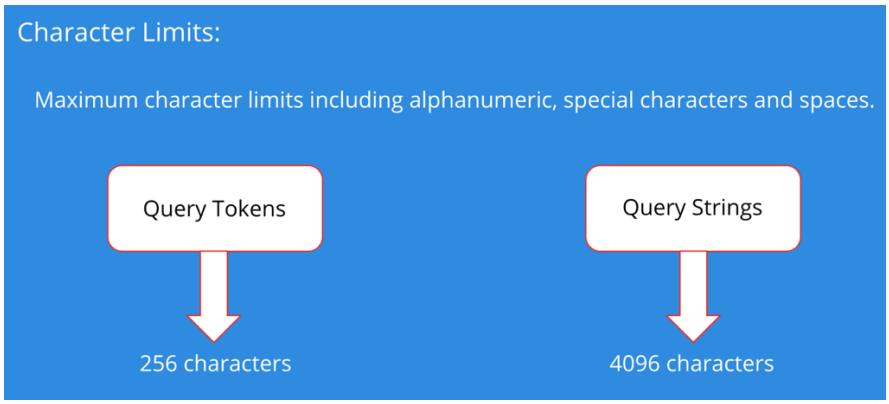
脆弱性データを表示するには「**Vulnerability(脆弱性)**」を、資産データを表示するには「**Asset(資産)**」を選択してください。そこから、データリストを簡単に閲覧し、詳細を確認できます



クエリのフォーマットに関する推奨事項

以下のビデオでは、クエリのフォーマットに関する推奨事項の一部について説明します。

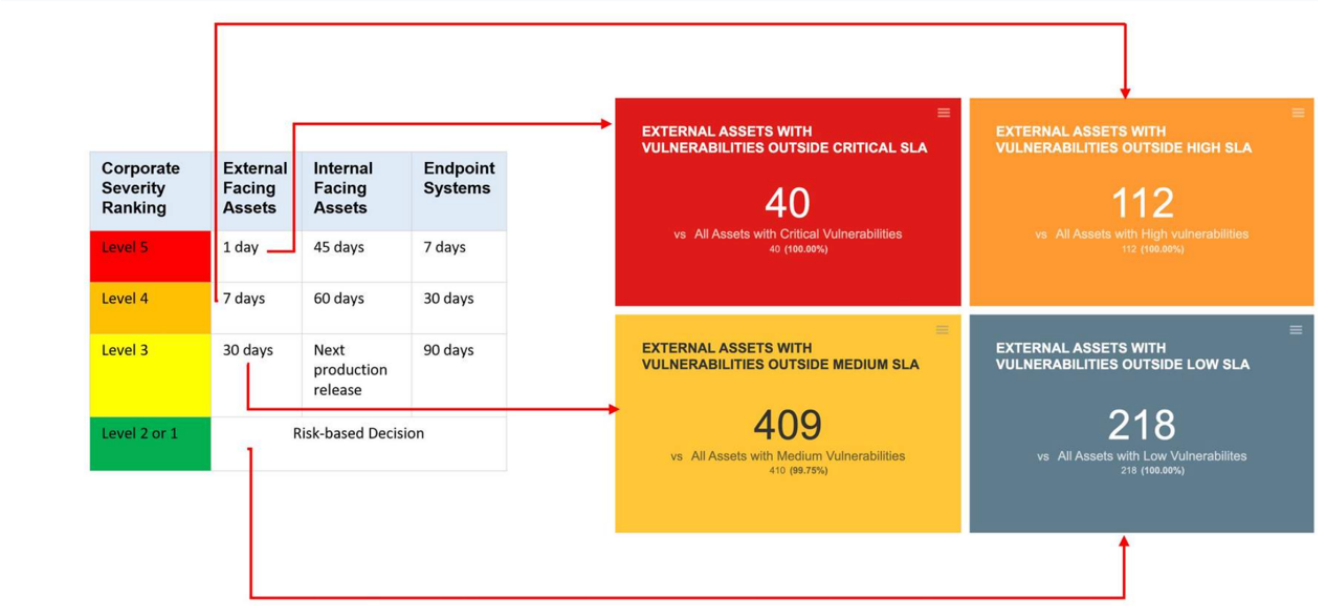




◉詳細情報と追加の推奨事項については、以下のリンクをご覧ください。
https://success.qualys.com/discussions/s/article/000005973

SLA と管理情報

これは、カスタム ウィジェットを使用して VM/VMDR ダッシュボード内で企業の修復 SLA を表す方法の例です。

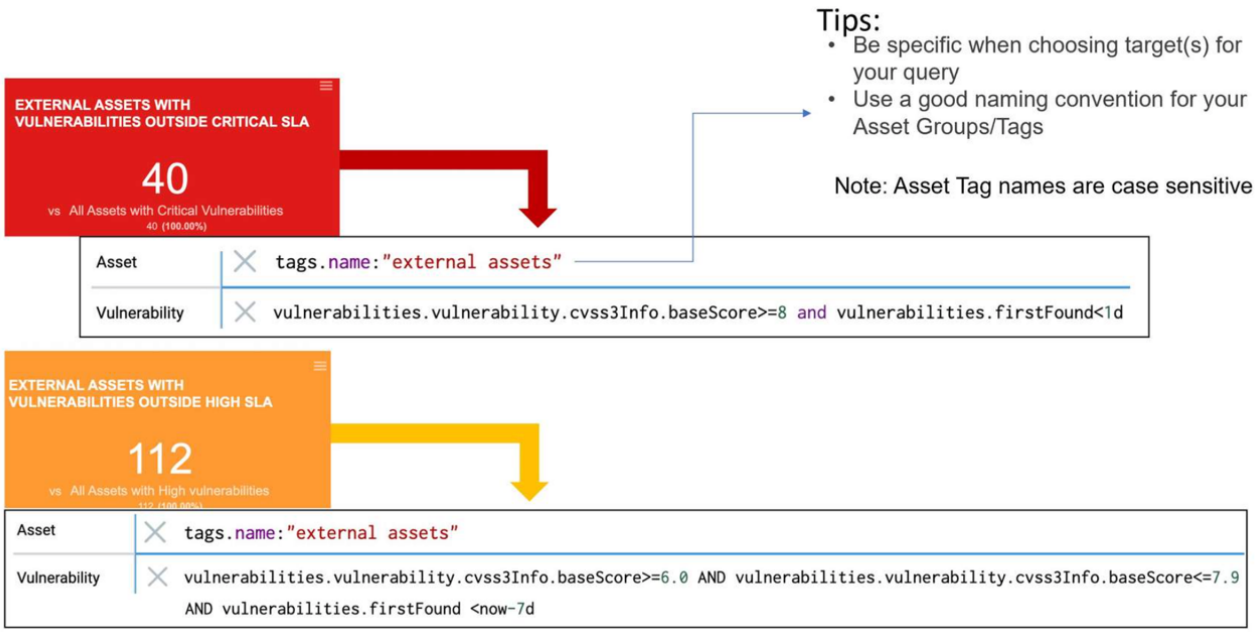


Critical かつ High SLA のクエリ

以下の画像は、前のトピックで説明したカスタム ダッシュボード ウィジェットの構築に使用されたクエリの一部を示しています。

最初のクエリは、CVSSv3 ベース スコアが 8 以上の脆弱性があり、1 日以上前に最初に発見されたすべての外部向け資産を検索します。

tags.name:"外部資産
" AND vulnerabilities.vulnerability.cvss3Info.baseScore>=8.0 AND vulnerabilities.firstFound<now-1d



2 番目のクエリは、CVSSv3 ベース スコアが 6 以上 7.9 以下の脆弱性があり、7 日以上前に最初に発見されたすべての外部向け資産を検索します。

tags.name: "External
Assets" **AND** vulnerabilities.vulnerability.cvss3Info.baseScore>=6.0 AND vulnerabilities.vulnerability.cvss3Info.baseScore<=7.9 AND vulnerabilities.firstFound <now-7d
Qualys では、Qualys アカウント内の IT 資産を整理・管理するために**アセットグループ**や**アセットタグ**を使用する場合、**適切な命名規則の使用を推奨**しています。また、レポートの対象を選択する際も、具体的な名前を付けることをお勧めします。また、アセットタグ名は大文字と小文字が区別されることにご注意ください。

◉資産タグの使用開始の詳細については、以下のリンクを参照してください。
https://qualysguard.qualys.com/qwebhelp/fo_portal/host_assets/tags_asset_tagging.htm（新しいタブで開きます）
サイバーセキュリティ資産管理（CSAM）にご登録ください（新しいタブで開きます）資産タグの設定と使用方法について詳しく学習するための自習型トレーニング。

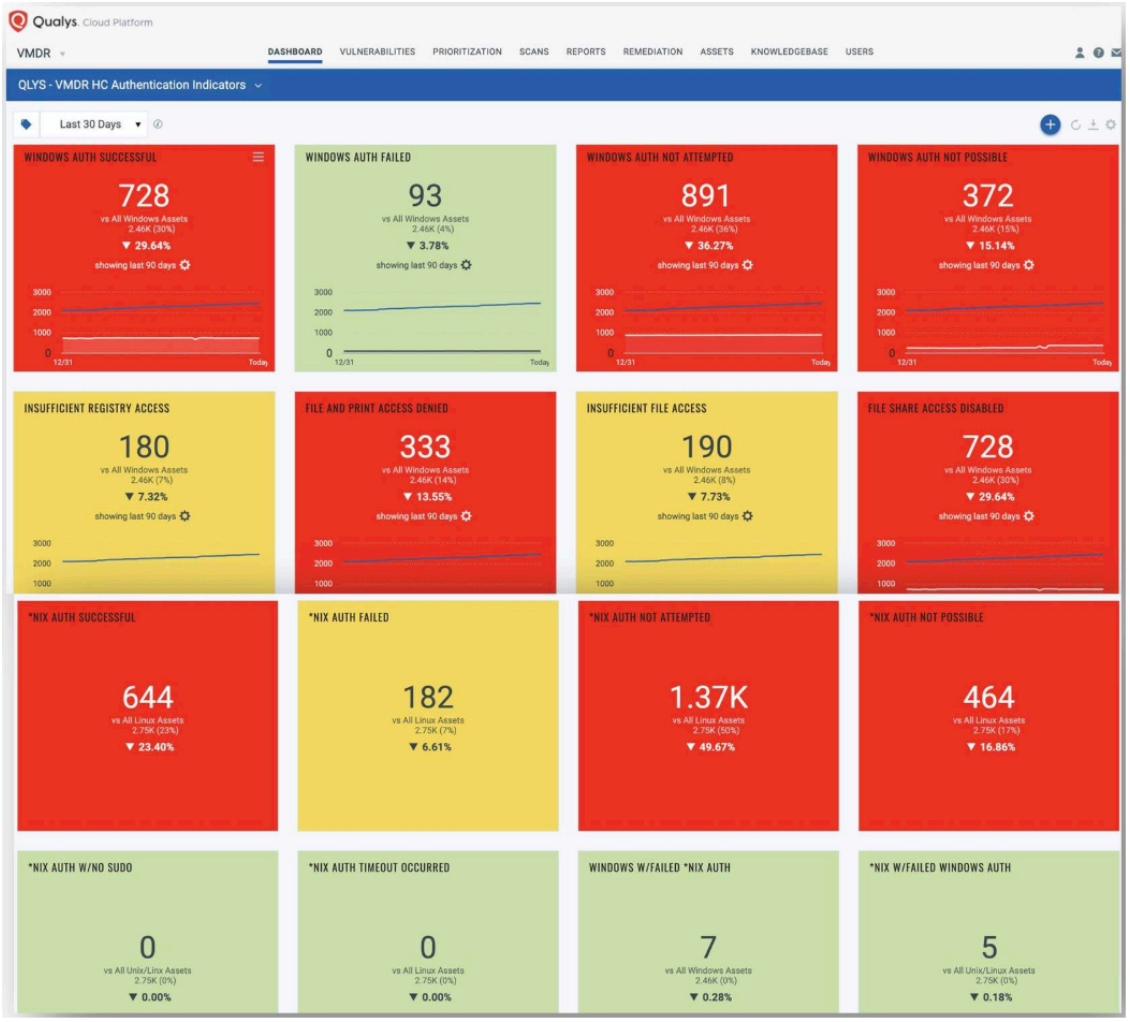
ダッシュボードウィジェットを使用した認証ステータスの追跡

ダッシュボードを使用すると、Qualys スキャンの認証管理をより積極的に行うことができます。さまざまなテクノロジーにおける認証の成功と失敗の KPI を、素早く簡単に確認できます。

認証ダッシュボード:

- 詳細を掘り下げることができる
- 自動的に更新される
- 認証レポートと比較して、認証失敗に関するより詳細な情報を提供する

認証ダッシュボードと認証レポートは互いに補完し合います。



◉Windows 認証管理用の事前構築された VM/VMDR ダッシュボード JSON ファイルは、次のリンクから入手できます。https://success.qualys.com/discussions/s/article/000006159

ダッシュボードのベストプラクティス

ダッシュボードにデータを入力するために使用されるクエリは、セキュリティ ポリシーとスキャン ルーチンと一致している必要があります。

毎週スキャンする場合は、クエリで「 **now-7d** 」を使用します (例: vulnerabilities.firstFound: now-7d)。

Qualys コミュニティには、すぐにインポートできるダッシュボードがいくつか用意されています。入手するには、Qualys コミュニティにアクセスしてください。（新しいタブで開きます） 。

コミュニティに投稿されたダッシュボードとウィジェットは Qualys アプリケーションモジュール固有のものであり、アプリケーションモジュール間で互換性がないことに注意してください。AssetView、Global Asset Inventory、ThreatProtect、CloudAgent、VM/VMDR などのダッシュボードは互いに独立しています。

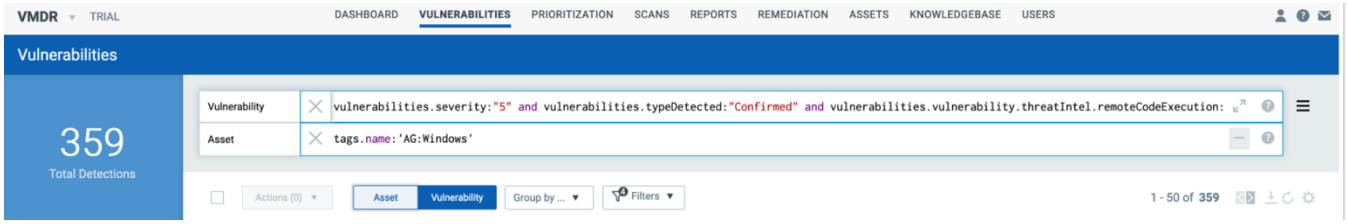
過去 30 日間にスキャンされていない資産、過去 7 日間に修正された脆弱性の合計など、特定のメトリックの変動を監視する必要がある場合は、トレンド グラフを使用する必要があります。

ダッシュボードは常に最新のスキャン結果を収集するため、古いホスト スキャン結果データを消去することが重要です。

◉ダッシュボードのベストプラクティスの詳細については、
https://success.qualys.com/discussions/s/article/000005976 の FAQ を参照してください。

ダッシュボードにウィジェットを追加する

以下のビデオでは、ダッシュボードにウィジェットを追加する方法を説明します。

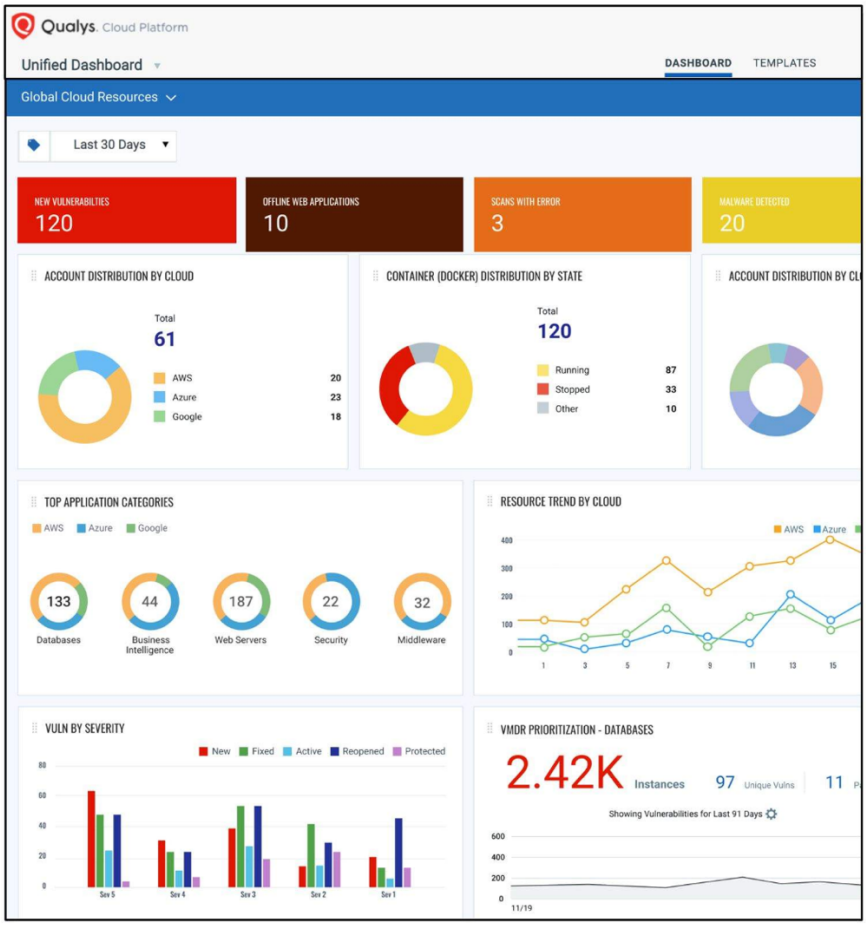


統合ダッシュボードの紹介

- 統合ダッシュボード（UD）は、すべての Qualys アプリケーションの情報を 1 か所に集めて視覚化します。
- UD は、既存のダッシュボード機能を強化するために他のすべての製品で消費および使用されるプラットフォームサービスとともに、強力な新しいダッシュボードフレームワークを提供します。
- ウィジェットビルダーを使用してダッシュボードを即興的に作成し、すべての製品で統一することができます。

Qualys 統合ダッシュボードには次の機能があります。

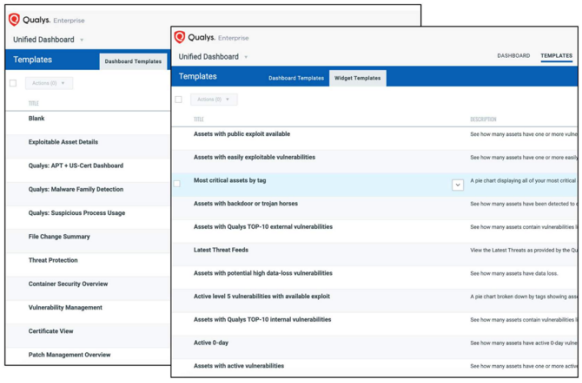
- データの視覚化とダッシュボードの作成/管理の使いやすさ
- クロスデータ視覚化のためのさまざまなモジュールからのウィジェット作成
- 最近のクエリからウィジェットを保存、管理、表示、作成する機能
- ウィジェットの簡単な複製–画面全体をフルワイドに活用
- ウィジェットから別のアプリケーションへの簡単な切り替え
- ダッシュボードから別のダッシュボードに簡単に切り替え可能
- あらゆるタイプのデバイスに対応するレスポンシブ UI
- ウィジェットとダッシュボードに、より強化された説明テキストを提供する機能
- 追加のグループ化
- 複数列のサポート
- 多次元グループ化



◉Qualys アカウントで統合ダッシュボードを有効にする方法については、以下をご覧ください。
https://success.qualys.com/discussions/s/article/000006183

テンプレートライブラリ

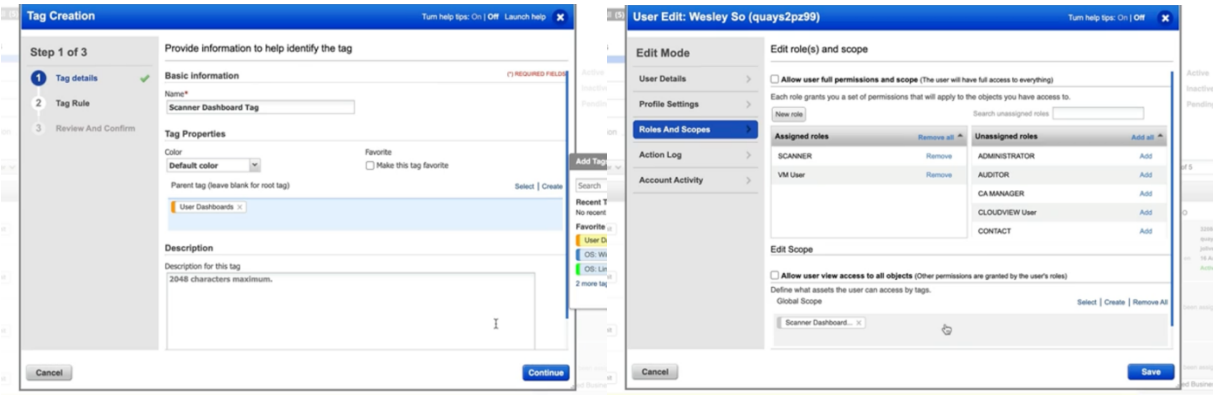
統合ダッシュボードを使用すると、セキュリティ チームは組織の脆弱性や現在のパッチ ポスチャの内訳などの IT 資産インベントリを 1 か所で確認できます。
統合ダッシュボードは、Global Asset View (GAV)、CyberSecurity Asset Management (CSAM)、EDR、脆弱性管理、パッチ管理、その他多くのウィジェットと統合的かつ動的に連携し、企業の単一ビューを提供します。
ダッシュボードとウィジェット テンプレート セレクターには、クロスデータ視覚化用のテンプレートを選択できる複数のアプリケーションが表示されます。



- パッチ管理、VMDR、EDR との統合により迅速なアクセスが可能。その他のアプリの統合もロードマップで予定されています。
- テンプレートセレクターを使用して、複数のすぐに使用できるダッシュボードとウィジェットを活用します。

Qualys ユーザーとダッシュボードを共有する

以下のビデオでは、ダッシュボードを Qualys ユーザーと共有する方法を説明しています。



修復の優先順位付け

- 脆弱性を特定したら、修復を優先するのが最善です。
- 最初にどの脆弱性を修正するかを決定するために使用できるパラメータがいくつかあります。
- 一般的に使用される方法には、Qualys の重大度ランキング、CVSS ベーススコア、リアルタイム脅威指標などがあります。

Qualys 重大度ランキング

Qualys の重大度評価を使用し、優先度の高い脆弱性から順に修正を優先していくのが、一般的に用いられるアプローチです。これには重大度 4 および 5 の脆弱性も含まれます。

次のような他の要素も含めることができます。

- 利用可能なエクスプロイトはありますか?
- 関連するマルウェアはありますか?

- 資産はどの程度重要ですか?
- コンプライアンスに影響しますか?

CVSS ベーススコア

優先順位を付ける別の方法は、CVSS スコアを確認することです。

以下を使用したり、参照したりできます:

- CVSS ベーススコア
- CVSS 一時スコア

リアルタイムの脅威指標

Qualys Threat Protection は、リアルタイムの脅威インジケーター（RTI）を提供します。

修復の優先順位を付けるには、RTI を使用できます。
これらの RTI は、ゼロデイ攻撃やサービス拒否攻撃などの外部の脅威ベクトルと脆弱性を関連付けます。

脅威保護

脆弱性の深刻度レベルは、脆弱性が悪用された場合の影響度を示します。深刻度は脅威そのものと同じではありません。例えば、深刻度の高い脆弱性に既知の脅威が関連付けられている場合、それは差し迫った脅威であり、可能な限り速やかに修正する必要があります。
脅威保護には、既知の脅威のライブフィードが含まれており、それらを資産と関連付けます。脅威保護により、脆弱性だけでなく、脅威に関連する資産を特定できます。これにより、リスクが高く、複数の脅威が関連付けられている資産を優先的に管理できます。

脅威保護:

- 最新の脅威に最もさらされている資産を特定する
- 最も大きなリスクをもたらす脆弱性を特定する
- 脆弱性データを優先順位付けすることで、次のことが可能になります。
  - 重大な脅威を迅速に修復
  - 脅威への露出を減らす*
- これらの脆弱性は、リアルタイム脅威指標（RTI）と呼ばれる正確なカテゴリに分類されます。

◉侵害の大部分は既知の脆弱性の悪用によって発生することに注意してください 。

脅威フィードのソース

Threat Protection で使用される脅威データ サブスクリプションには次のものが含まれます。

- エクスプロイトソース

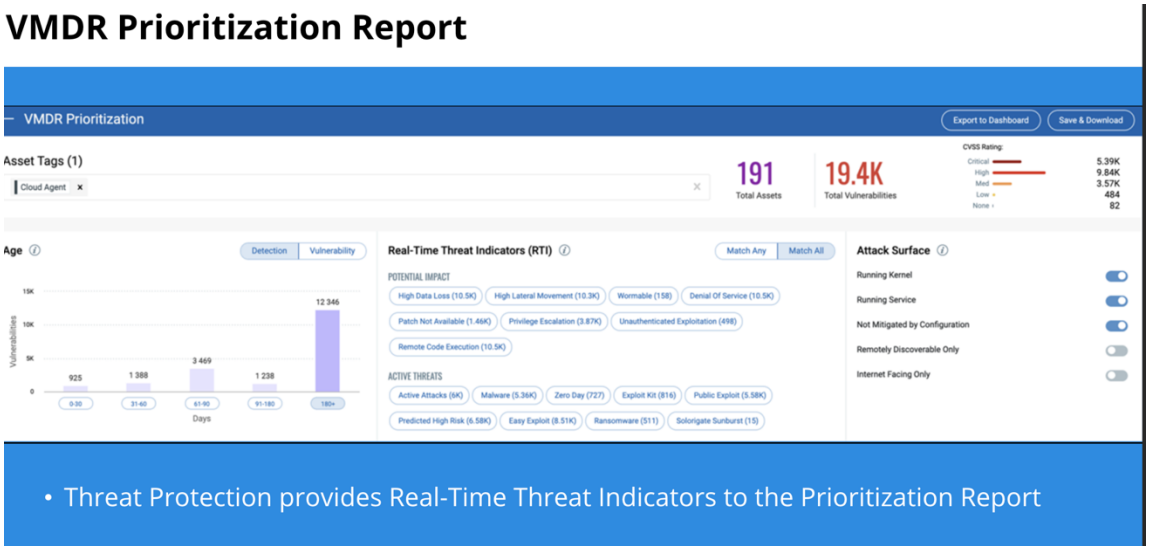
Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosporus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

- マルウェアのソース

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

VMDR 優先順位付けレポート

VMDR 優先順位付けレポートは、資産コンテキスト、脆弱性の年齢、脅威インテリジェンス、攻撃対象領域のダイナミクスなど、複数の要素を使用して脆弱性の優先順位付けとパッチ適用を行うために設計されています。
以下のインタラクティブ ビデオでは、修復レポートを作成してパッチ適用アクティビティの進行状況を監視する方法について説明します。



報告のベストプラクティス

Qualys のテンプレートベースのレポートは、サブスクリプションからすべての脆弱性をエクスポートするのではなく、読みやすく、理解しやすく、優先順位を付けやすいレポートを生成します。

Qualys のテンプレートベースのレポートは、大規模なデータのエクスポートには対応していません。Qualys は、サブスクリプションからすべての脆弱性をエクスポートするなど、大規模なデータのエクスポート用の API を提供しています。
考慮すべきベストプラクティスをいくつか以下に示します。

1. 環境内でデータの一貫性を維持するために、適切な資産ハウスキーピングとデータ衛生のプラクティスを実装します。
2. 最良の結果を得るには、スキャンベースのレポートではなく、ホストベースのレポート(対象となる資産グループや資産タグ、および焦点を絞った検索リストを含む)を使用します。
3. レポートルーチンはスキャンルーチンと一致する必要があります。つまり、毎週スキャンする場合は毎週レポートします。
4. 傾向分析の結果を改善するために、長期にわたって一貫したレポート構造を維持します。
5. レポート利用者と頻繁に連携し、レポートをメンテナンス プロセスと最も適切に連携させる方法を評価します。
6. Qualys は、サブスクリプションからすべての脆弱性をエクスポートしてハイブリッド レポート アーカイブ プログラムを作成するなど、大規模なデータのエクスポート用の API を提供します。
7. Qualys API とサードパーティ製アプリケーションとの統合もご利用いただけます。例えば、Qualys App for Splunk Enterprise は、TA-QualysCloudPlatform 経由で Qualys アカウントから脆弱性とコンプライアンス検出データを取得し、Splunk に取り込むことで、検索やレポート作成を容易にします。

◉環境内の関連する指標を追跡し、すばやく見つけたり確認したりできるようにする、焦点を絞った検索リストについては、以下のリンクを参照してください。
https://success.qualys.com/discussions/s/article/000006215（新しいタブで開きます）
レポートのベスト プラクティスに関する FAQ を確認するには、以下のリンクにアクセスしてください。
https://success.qualys.com/discussions/s/article/000005984

報告哲学

レポートは、環境内の修復を促進するためにも、パッチ適用プログラムの進捗状況を確認するための監査としても使用できます。スキャンレポートテンプレートは、含める技術データの並べ替えや優先順位付けの柔軟性が最も高いため、最も人気のあるレポートです。また、環境に必要なパッチを示すパッチレポートを作成することもできます。ベストプラクティスは、パッチで並べ替えることです。

修復

レポートを使用してセキュリティと運用アクティビティを推進します。

- パッチごとに分類されたパッチレポートは、パッチを配布する運用チームにとって優れた情報源となります。
- スキャンレポートテンプレートを使用して、優先度の高い/緊急の脆弱性、結果、パッチを含む詳細なレポートを作成します。

監査パッチ適用プログラム

脆弱性管理プログラムの進捗状況を評価するには、役立つメトリックを含むレポートを使用します。

- ダッシュボードでは高レベルのデータを見ることができます。
- 修正された脆弱性レポートには、指定された期間内に修正された脆弱性がリストされます。
- 修復レポートは、パッチ適用プログラムの有効性を測定するために使用できます。
- エグゼクティブレポートなどの**トレンドレポート**を使用して、「**資産グループ別のビジネスリスクの推移**」を評価します。

レポート生成

以下のレポート例を考えてみましょう。

トレンドグラフを含むレポートを作成したいとします。レポート内のグラフによって出力ファイルのサイズはそれほど大きくなりませんが、トレンドグラフを作成するために Qualys プラットフォームが処理しなければならない、各資産の検出ごとの遷移データの量は数倍に増加します。さらに、検出履歴が長く、遷移量が多い場合、Qualys プラットフォームは同じ検出数に対してより多くのデータを処理する必要があります。これは、レポート生成の成功率に重大な影響を与える可能性があります。

提案：トレンド期間を短縮する、脆弱性フィルタリングを適用する、資産フィルタリングを使用するなどの対策を講じてください。これらの対策により、Qualys プラットフォームのデータ量が削減され、成功率が向上します。

レポート生成に影響する属性:

- プラットフォームが処理する必要があるデータの量（傾向）
- 出力ファイル内のデータ量:
  - 資産数
  - 検出数

提案：

トレンド期間を短縮し、重点的な検索リストを使用して脆弱性をフィルタリングし、重点的な資産ターゲットを使用する

それ以外の場合は、データエクスポート用の API を検討してください。

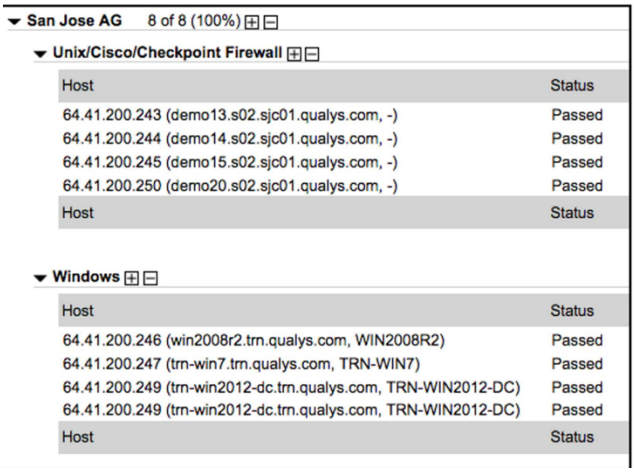
認証レポートの生成

認証レポートを実行する際は、まずレポート形式を定義する必要があります。「スケジュールされた」認証レポートでは、PDF ファイル形式が一般的に使用されます。その他のオプションとして、HTML、CSV、XML があります。

次に、レポート対象となる資産を選択します。ビジネスユニット、資産グループ、IP、または資産タグのいずれかを選択できます。ここで選択したオプションによって、レポートデータのグループ化方法が決まります。

選択したターゲットのホスト アセットが、最後の認証試行のステータス（PASS または FAIL）とともにリストされます。

- 認証レポートには、スキャンされた各ホストの認証ステータスが表示されます。
- 合格
- 失敗
- 権限が不十分なため合格
- 未試行
- 認証スキャンを実行した後、このレポートを実行します。



San Jose AG　8 of 8 (100%)

Unix/Cisco/Checkpoint Firewall

Host	Status
64.41.200.243 (demo13.s02.sjc01.qualys.com, -)	Passed
64.41.200.244 (demo14.s02.sjc01.qualys.com, -)	Passed
64.41.200.245 (demo15.s02.sjc01.qualys.com, -)	Passed
64.41.200.250 (demo20.s02.sjc01.qualys.com, -)	Passed
Host	Status

Windows

Host	Status
64.41.200.246 (win2008r2.trn.qualys.com, WIN2008R2)	Passed
64.41.200.247 (trn-win7.trn.qualys.com, TRN-WIN7)	Passed
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)	Passed
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)	Passed
Host	Status

脆弱性レポートを作成する手順

カスタム脆弱性レポートを作成する前に、まず対象となるホスト資産を評価し、最終的に様々な知見を生み出すホストデータを収集する必要があります。現在、Qualys はホスト評価を実行する 2 つの方法を提供しています。

- Qualys Scanner Appliance を使用してスキャンを開始する
- Qualys Cloud Agent をホストアセットに直接導入する

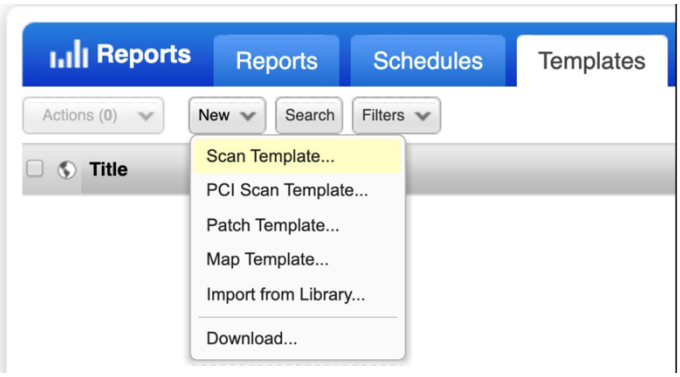
スキャナまたはエージェントを使用してホストデータを収集したら、カスタムレポート設定を含むレポートテンプレートを構築または作成します。ニーズを満たすレポートテンプレートが完成したら、それを使用してホストアセットのレポートを生成します。レポートを生成する前に、スキャナアプライアンスまたはエージェントによるデータ収集を完了しておく必要があることに注意してください。

1. ホスト評価を実行します。

- Qualys スキャナアプライアンス
- Qualys クラウドエージェント

2. レポート テンプレートを使用してレポートを実行します。

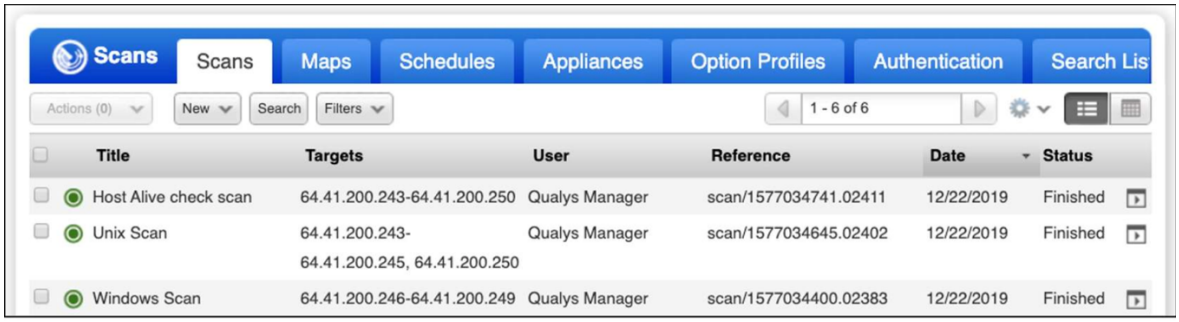
- あらかじめ定義されたレポートテンプレートを使用する
- カスタムレポートテンプレートを作成する



スキャンに基づく所見(Scan-Based Findings)

脆弱性管理アプリケーション内で「スキャン」メニューをクリックし、「スキャン」タブをクリックすると、すべての SCAN データを表示できます。これらはスキャンベースの検出結果です。Qualys アカウント内で実行されたすべての脆弱性スキャンがここに表示されます。もちろん、削除されたスキャンは含まれません。特定の時間（特定の日付）に収集されたデータと検出結果に焦点を当てたレポートを作成する場合は、スキャンベースの検出結果を使用する必要があります。

- スキャンベースの結果（または「生の」スキャンレポート）は、「スキャン」タブにあります。
- スキャンベースの調査結果は、特定の時点をターゲットにした「スナップショット」レポートに最適です。

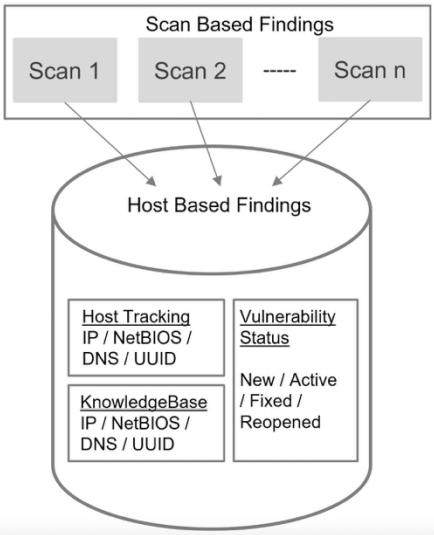


スキャンベースのレポートの重要なポイント

1. スキャンベースの検出結果は、Qualys スキャナアプライアンスでスキャンされたアセットに対してのみ生成されます。Qualys Cloud Agent は自動継続スキャンモードであるため、ホストベースの検出結果のみを生成します。
2. スキャンベースの検出結果には、資産の特定時点のスナップショットが含まれます。そのため、脆弱性のステータスは表示されません。
3. ほとんどの場合、ホストベースの調査結果を使用することになります。これは、資産の最新の状態に焦点を当てています。
4. スキャンベースの結果は、資産の事後的な状態を表示したり、1 日にホストをスキャンするのにかかった時間、認証が成功したか失敗したか、どの認証プロトコルが使用されたか、検出されたホップの数など、トラブルシューティングの目的で時々使用されます。

ホストベースの調査結果

- すべてのスキャンベースの検出結果は、ホストベースの検出結果と呼ばれる別のバケットに注ぎ込まれます。
- ホストベースの検出結果データベースは、完了したスキャンからデータを収集し、各ホスト資産に対して選択した「追跡方法」に従って、検出された各脆弱性をインデックス化します。
- ホストベースの検出結果を使用すると、任意のホスト資産の脆弱性履歴を表示できます。スキャンベースの検出結果とは異なり、ホストベースの検出結果では、任意のホスト上のあらゆる脆弱性のステータス（新規、アクティブ、修正済み、再オープンなど）を追跡する脆弱性「トレンド」レポートを作成できます。



ホストベースの調査結果

- 各ホストの脆弱性履歴を提供します
- トレンドレポートの作成に必要
- 脆弱性のステータスを追跡：新規/アクティブ/修正済み/再開

ホストベースの調査結果に影響を与える要因

ホストベースの調査結果を扱うときは、次の要因による影響に注意してください。

- 認証モードの変更
- 対象となるサービスポートの変更、および
- 宿主の「生死」ステータスの変化

ホストベースの検出結果を扱う際に考慮すべきもう 1 つの要素は、**ホスト名または IP アドレスの変更**です。ホストが検出された脆弱性を追跡するためにホスト名または IP アドレスを使用するように設定されている場合、ホスト名または IP アドレスが変更されると、脆弱性が誤ったホストに関連付けられる可能性があります。ホスト名または IP アドレスが変更された直後に、ホストベースの検出結果を消去することは、一般的に行われている方法です。

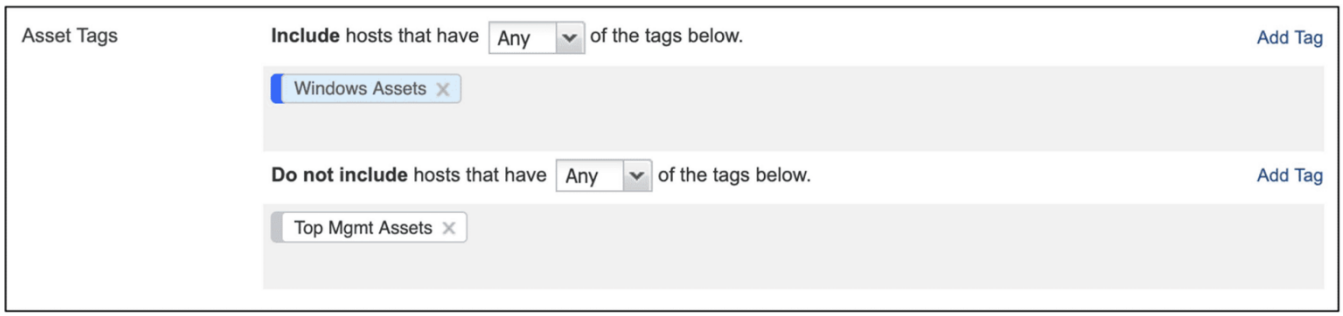
脆弱性の検出結果に矛盾がある場合（検出結果が ACTIVE と表示されているのに、FIXED と表示されることを期待していた場合など）は、**追加のスキャンを実行**することで解決できることに留意してください。

このような矛盾を分析する際には、疑わしい所見の「**最終検出日(last detected)**」と**報告日**を比較してください。最終検出日と報告日の間に大きな隔たりがある場合は、追加の検査が必要である可能性があります。

レポートソース - 資産タグ

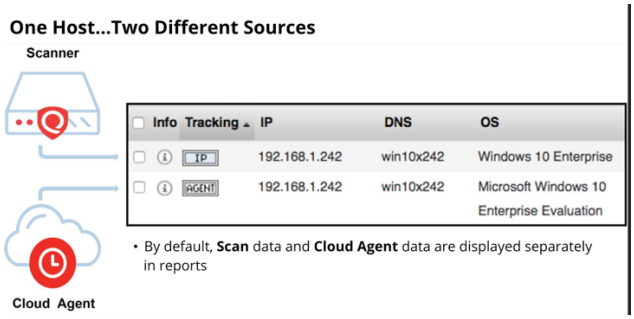
アセットタグはレポートのターゲットとして使用できます。アセットタグを使用すると、ホストの IP アドレス変更を気にすることなく、ホストをターゲットにすることができます。

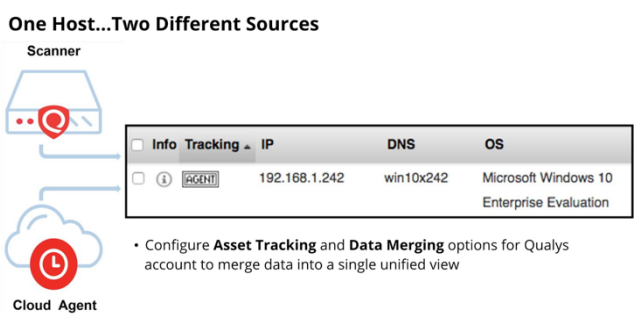
- アセットタグを使用すると、ホストの追加や削除によってネットワークが常に変化している場合でも、特定の基準に一致するホストを含めることができます。
- たとえば、すべての Windows ホストまたはポート 443 が開いているホスト
- アセットタグは、アセットグループや IP 範囲がサポートされていない場合、または追加の作業なしではサポートされない場合を含めたり除外したりできます。



1 つのホストと 2 つの異なるソース

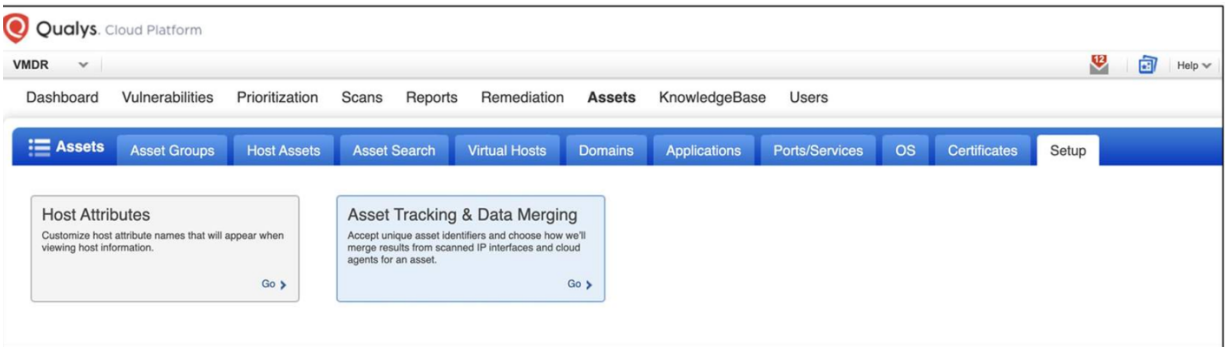
以下のビデオでは、2 つの異なるデータ ソースを使用して 1 つのホストをスキャンした場合のレポートの表示方法について説明します。





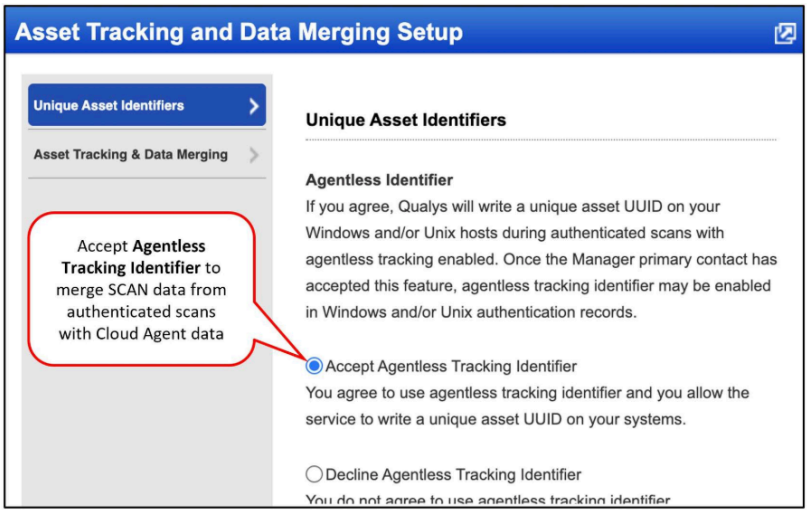
資産追跡とデータ統合

- アセットトラッキングとデータマージ機能により、スキャン結果をクラウドエージェントデータとマージして、ホストベースのスキャンレポートでホストのレコードを 1 つ表示できます。
- 開始するには、サブスクリプションのプライマリマネージャユーザーが VM または VMDR アプリケーションでこれらのオプションを承認する必要があります。

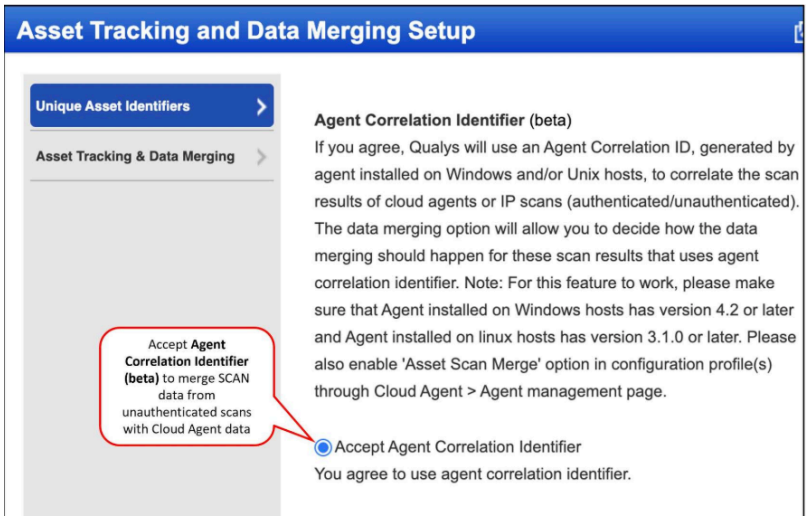


クラウドエージェントによるホストのスキャン

- 一意の識別子を使用して資産を追跡するためのオプションは、エージェントレス追跡識別子とエージェント相関識別子です。



エージェントレス追跡識別子(Agentless Tracking Identifier)機能を使用して、スキャンされた IP インターフェースと Cloud Agent アセットのエージェント VM スキャンからの認証された脆弱性スキャン結果をマージします。



エージェント相関識別子(Agent Correlation Identifier)を使用して、スキャンされた IP インターフェースと Cloud Agent アセットのエージェント VM スキャンからの認証されていない脆弱性スキャン結果をマージします。

◉エージェント相関識別子と認証されていないスキャンのマージ機能の詳細については、次のリンクを参照してください。

https://success.qualys.com/discussions/s/article/000006550（新しいタブで開きます）

どちらか一方、または両方の識別子を使用できます。アカウントで両方の固有のアセット識別子を受け入れることで、統合の可能性が最大限に高まります。

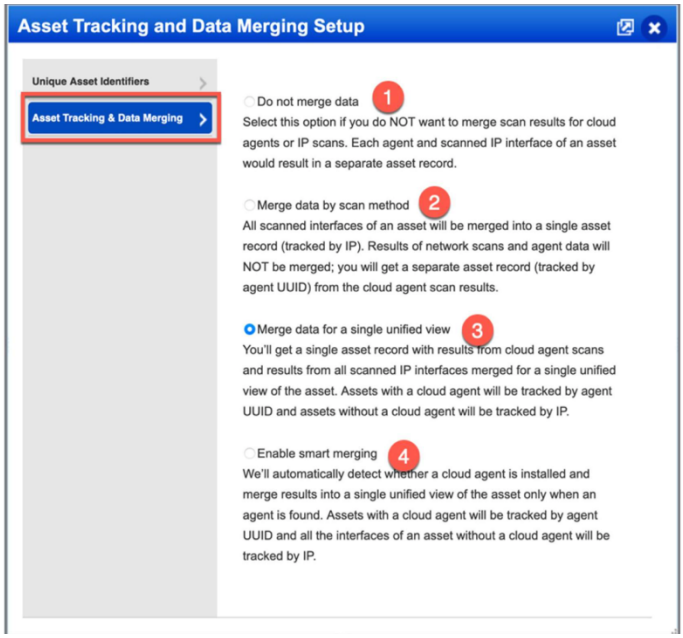
承認後は、エージェントレス追跡識別子またはエージェント相関識別子を使用してスキャンを開始する前に、追加の手順を完了する必要があることに注意してください。

データの結合

次のステップは、適切なデータマージオプションを設定することです。**オプション 3 を**選択すると、SCAN データと AGENT データが単一の統合ビューにマージされます（下図参照）。

以下に結合オプションを示します。ニーズに応じて適切なデータ結合方法を選択してください。

マージオプション:



1. **Do not merge data(データを結合しない)** エージェントから収集されたデータは、スキャナアプライアンスによって収集されたデータとは別に表示されます。IP トラッキングが有効になっているホストでは、スキャンされたすべてのインターフェースのアセットレコードが個別に表示されます。
2. **Merge data by scan method(スキャン方法別にデータをマージ)** エージェントレス追跡識別子と組み合わせると、オプション 2 は、スキャンされたすべてのインターフェース（IP 追跡が有効になっているインターフェース）から収集されたデータを単一の資産レコードにマージします。
3. **Merge data for a single unified view(データを統合して単一の統合ビューに表示)**エージェントから収集されたデータは、スキャナアプライアンスから収集されたデータと統合され、単一の統合ビューに表示されます。
4. **Enable smart merging(スマートマージを有効にする)** エージェントがインストールされているホストでは、オプション 3 が自動的に選択されます。エージェントがインストールされていないホストでは、オプション 1 が使用されます。

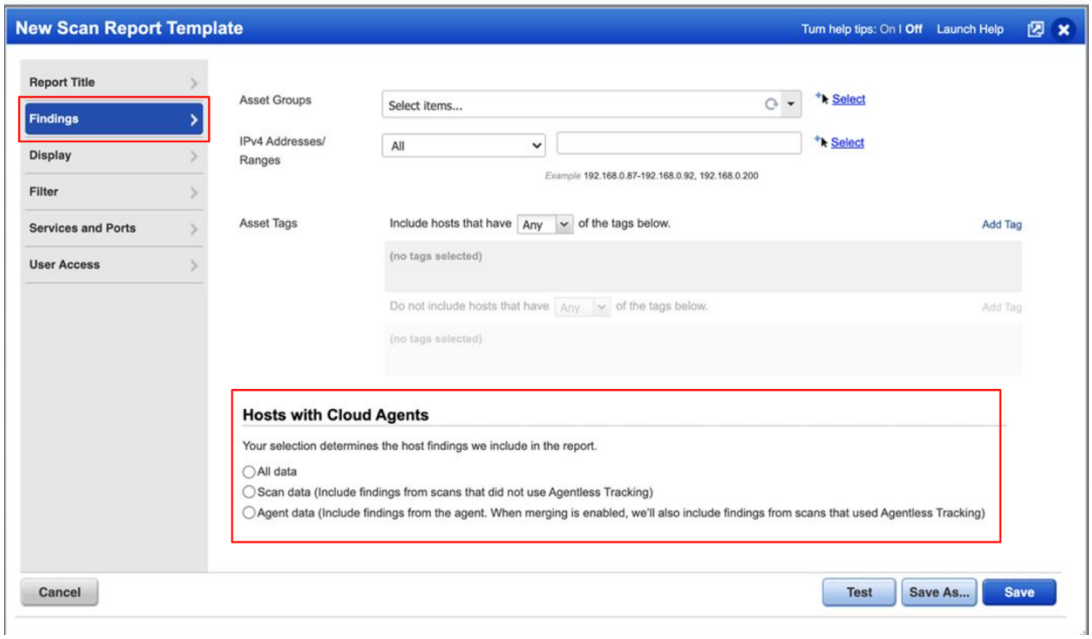
データ結合オプション

以下の表は、Qualys アカウントで設定されたデータ結合オプションに応じて、1 つ以上の IP インターフェースからのスキャン データが Cloud Agent データと結合されるシナリオを示しています。

データ結合オプション	SCAN データと AGENT データをマージする	複数のホストインターフェースを統合する	説明
データを結合しない	いいえ	いいえ	エージェントまたは IP スキャンのスキャン結果をマージしないでください。
スキャン方法によるデータの結合	いいえ	はい	一意の追跡識別子（エージェントレス追跡 ID またはエージェント相関 ID）が必要です。資産のすべての IP スキャンインターフェースは、単一の資産レコードに統合されます（デフォルトでは DNS と NetBIOS の追跡）。
単一の統合ビューにデータを統合	はい	はい	すべてのエージェント スキャンの結果と、スキャンされたすべての IP インターフェイスの結果が、資産の単一の統合ビューに統合されます。
スマートマージを有効にする	はい	はい	エージェントの存在に応じて、オプション 1 または 3 が自動的に選択されます。

Cloud Agent 搭載ホストのレポート オプション

以下のビデオでは、Cloud Agent を使用したホストの統合ビューを有効または無効にするときに使用できるさまざまなレポート オプションについて説明します。



エージェントスキャンマージシナリオ

Cloud Agent データとスキャンデータをマージする際、最初にスキャン（認証済み/未認証）を実行したか、スキャンの前に Cloud Agent データが収集されたかによって、結果が異なる場合があります。これらのシナリオによって結果が異なる場合があります。考慮すべきシナリオをいくつかご紹介します。

- エージェント収集とそれに続く認証されていないスキャン

- 認証されていないスキャンとそれに続くエージェントコレクション
- エージェント収集とそれに続く認証スキャン
- 認証スキャンとそれに続くエージェントコレクション
- EC2 ホスト - エージェント収集とそれに続く内部 EC2 スキャン
- EC2 ホスト - 最初にアプライアンス スキャン（IP 追跡レコードとエージェント追跡レコードなし）
- EC2 ホスト - エージェント収集が最初（IP 追跡レコードとエージェント追跡レコードなし）

現在の重複レコードはどうなりますか?

マージは設定時点から実行されます。Qualys は、以前の設定によって生成された IP 追跡アセットを遡及的にクリーンアップすることはありません。

また、一意の資産識別子と統合ビューが有効になっている場合、古いレコードが発生する可能性があります。それでも、スキャナはエージェントレス追跡識別子（認証失敗のため）またはエージェント相関 ID（ポートがブロックされている、QID 48143 がスキャンに含まれていないなど）を取得できません。

上記の条件が存在する場合、古いレコードを識別して削除する必要があります。

詳細については、次のドキュメントを参照してください。

エージェントスキャンマージケース（新しいタブで開きます）

VM のエンティティ ID を理解する（新しいタブで開きます）

エージェントレス識別子と統合ビューを有効にした古いレコードの識別

スキャンレポートテンプレート - 表示オプション

レポートを作成する際に共通して考慮すべき点は、対象読者を考慮することです。そのため、レポートを作成する際は必ず、「このレポートは誰のために作成するのか？」と自問自答してください。

このレポートを上級管理職と共有しますか？それとも、パッチ適用プログラムに参加するシステム管理者と共有しますか？当然、それによってレポートの内容が決まります。

次に尋ねるべき質問は、彼らは何を見る必要があるのかということです。

レポートはできるだけ簡潔にまとめることが重要です。もちろん、ご要望があればテンプレートに情報を追加することも可能です。

◉重要：

レポート生成の成功率は、Qualys クラウド プラットフォームが処理する必要があるデータの量と、出力ファイルに公開されるデータの量によって異なります。

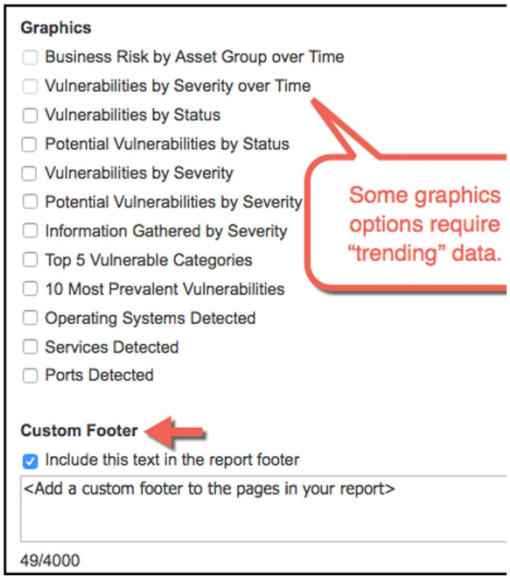
◉ベストプラクティス:

できるだけ効率的にレポートを作成するようにしてください。

グラフィック

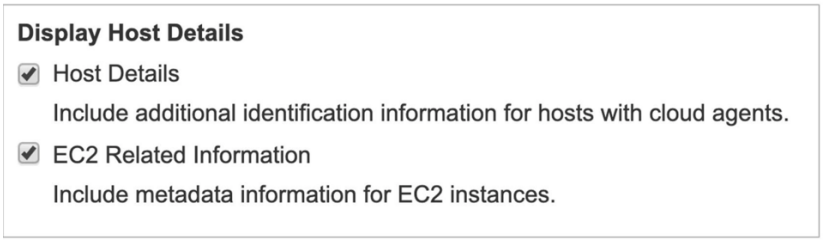
表示セクションで次に注目すべき項目はグラフです。レポートをよく見ると、チェックした内容の内訳を示すグラフが表示されていますか？
上位 2 つのグラフオプションを使用する場合は、一定期間にわたるホストベースの傾向分析結果を使用する必要があります。それ以外の場合、これらのオプションはグレー表示になります。
カスタムフッターを使用すると、レポートの下部に情報を配置できます。例えば、レポートを配布する際に、機密情報であることを関係者に知らせたい場合などです。

- グラフィックオプションを選択するときは、ターゲットオーディエンスを考慮してください。
- 一部のグラフィックオプションでは「傾向」データが必要です。
- 最大 4000 文字のカスタムフッターを追加します。



ホストの詳細を表示

次に、Cloud Agent ホストに関する情報については、ホストの詳細を選択する必要があります。
具体的には、エージェントホストのアセット ID が提供されます。これは、すべてのクラウドエージェントのアセットに関連付けられた一意の識別子です。



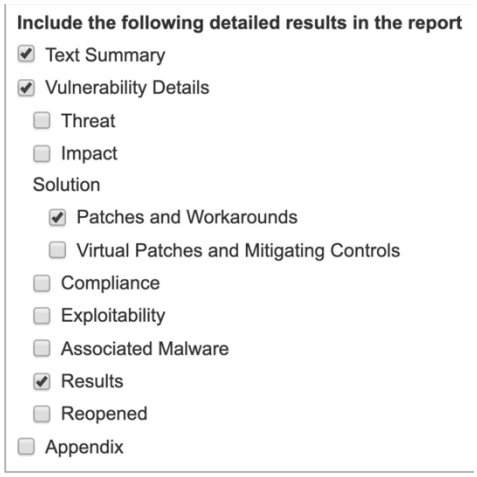
AWS EC2 アセットを対象とするレポートの場合は、「EC2 関連情報(EC2 Related Information)」チェックボックスをオンにします。　これは、EC2 ホストに関する重要な情報を提供します。パブリック DNS を使用している場合は、ここに表示されます。ホストの AMI も表示されます。これは重要な情報です。パッチ適用時に AMI レベルでパッチを適用すれば、その AMI から起動されたホストには脆弱性が存在しないからです。VPC のロケーションも確認できます。各インスタンスの状態（実行中、停止中、終了済みなど）も表示されます。プライベート DNS とインスタンスタイプも確認できます。

詳細な結果を含める

Qualys の脆弱性管理コースを受講したことがある場合は、すべての脆弱性または QID に多くの情報が含まれていることをご存知でしょう。
すべてのボックスをチェックすると、詳細の量とレポートのサイズが増加し、レポートの生成に必要な時間も長くなります。

- ほとんどの脆弱性レポートには、検出された脆弱性と推奨される解決策が含まれています。
- 脆弱性固有の証拠を表示するには、「結果」チェックボックスを選択します。

- 含める詳細を選択するときは、次の質問を自問してください。
- ターゲットオーディエンスは何を見る必要があるでしょうか?
- 当面の目的を達成するにはどのような情報が必要ですか?
- レポートに含める必要のある他の詳細は何ですか?



◉重要：
Qualys UI レポートは、サブスクリプションからすべての脆弱性をエクスポートするのではなく、人間が判読できるレポートを生成することを目的としています。

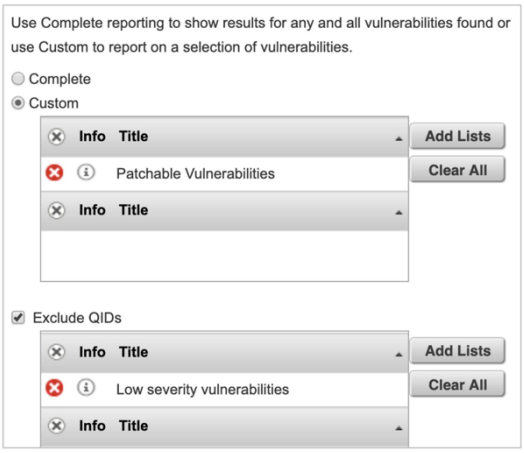
スキャンレポート – フィルターオプション

フィルター オプションを使用すると、特定のオペレーティング システムとともに QID の数とタイプを絞り込むことができるため、組織内のさまざまなチームに固有のレポートを作成できるようになります。

- フィルター番号と QID の種類
- 特定のオペレーティングシステムをフィルターする
- 異なるチームごとに個別のレポートを作成する

検索リストを使用してレポートをフィルタリングする

検索リスト(Search List)は、パッチ適用可能な脆弱性、深刻度の高い脆弱性、エクスプロイトが仕掛けられている脆弱性など、特定の脆弱性に焦点を当てるために使用できます。また、レポートから特定の脆弱性を除外することもできます。タグと組み合わせることで、非常にターゲットを絞ったレポートを作成できます。



●検索リストを使用して、レポートに含める特定の QID をフィルタリングします。例：パッチ適用可能なすべての脆弱性

●1 つ以上の検索リストを追加できます

●検索リストを使用して、特定の QID をレポートから除外することもできます。例: 重大度 1 および 2 のすべての脆弱性。

レポート生成

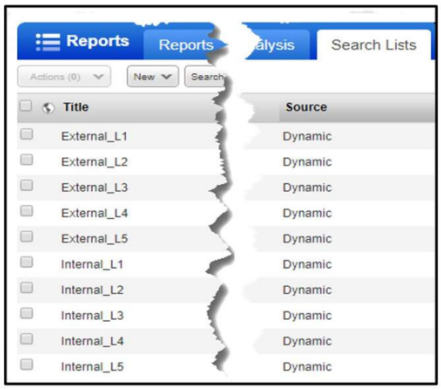
以下のビデオでは、マルウェアやランサムウェアに対する資産の露出を示すレポートを生成する方法を説明します。

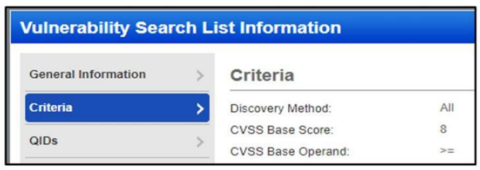
検索リストを使用した選択的レポート

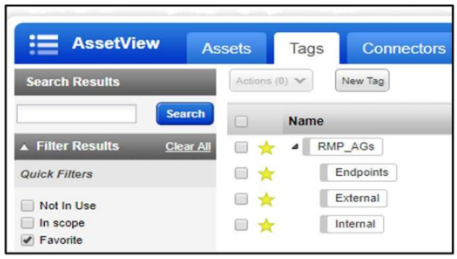
これは、検索リストを使用して企業の重大度ランキングを調整する方法の例です。
この例では、CVSS 基本スコアを使用して外部向け脆弱性の検索リストを作成し、CVSS 現状スコアを使用して内部向け脆弱性を検索します。資産はタグを使用して識別されています。

Corporate Severity Ranking	CVSSv* Score	Corporate Vulnerability Severity Evaluation Criteria
Level 5 (Critical)	8.0 – 10.0	The vulnerability may allow: • An attacker to assume remote administrator or root privileges • Exposure (full read and write access) of a host, application or backend database
Level 4 (High)	6.0 – 7.9	The vulnerability may allow: • An attacker to assume only user privileges, or perform a complete denial of service attack
Level 3 (Medium)	4.0 – 5.9	The vulnerability may allow: • An attacker to abuse or misuse a host or application, or perform a partial denial of service attack

Corporate Severity Ranking	External Facing Assets	Internal Facing Assets	Endpoint Systems
Level 5	1 day	45 days	7 days
Level 4	7 days	60 days	30 days
Level 3	30 days	Next production release; not to exceed 90 days	90 days



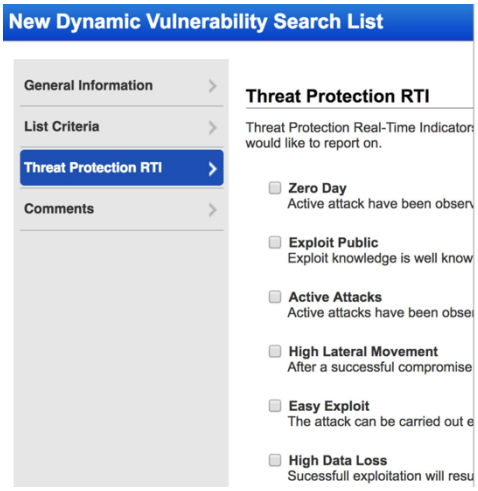




検索リストで RTI を使用する

Threat Protection RTI を使用して検索リストを作成できます。1 つの検索リストで複数の RTI を選択できます。オプションプロファイルと組み合わせることで、スキャンおよびレポートテンプレートを絞り込むことができます。

- **RTI を**使用して**検索リスト**を作成する
- これらの「**検索リスト**」は、スキャン、レポート、修復の目的で使用できます。



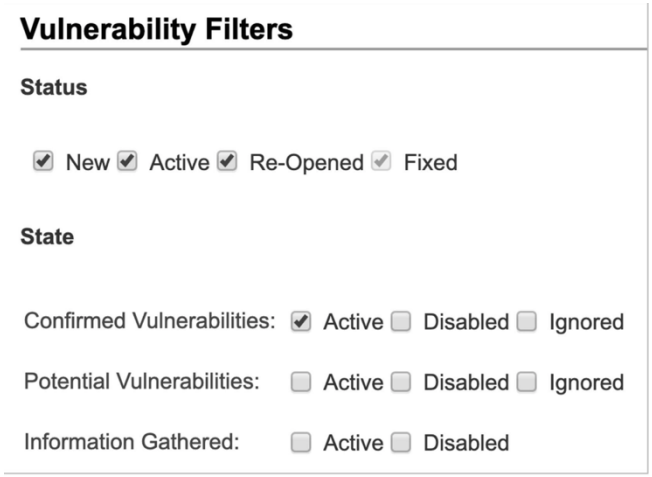
脆弱性フィルター

脆弱性フィルターを使用すると、レポートに表示する脆弱性のステータスを定義できます。
脆弱性には、次の 4 つのステータスのいずれかが設定されます。

1. 資産に脆弱性が初めて検出された場合、そのステータスは「**新規(New)**」になります。
2. 複数回検出された脆弱性の場合、そのステータスは**アクティブ(Active)**になります。
3. 脆弱性が検出されなくなると、そのステータスは**修正(Fixed)**になります。
4. 修正された後に再発見された脆弱性については、ステータスが**再度オープン(ReOpen)**になります。

修正された脆弱性を報告する場合は、調査結果の傾向オプションを有効にする必要があります。
脆弱性にはステータスに加え、状態も存在します。デフォルトの状態は「アクティブ」です。これは、脆弱性がアクティブにスキャンされ、レポートされていることを意味します。脆弱性はナレッジベースから無効化することもできます。無効化すると、スキャンレポートにおいてすべてのホストからグローバルに除外されます。
特定の理由により、脆弱性が一定期間無効化または無視される場合があります。これらの状況を報告する場合は、関連する状態オプションが必要となります。
無視される脆弱性とは、特定の資産上で無視される特定の脆弱性です。

- 脆弱性のステータスでレポートをフィルタリングします。
- 新規(New)
- アクティブ(Active)
- 再開(ReOpen)
- 修理済み(Fixed)
- 脆弱性の状態別にレポートをフィルタリングします。
- 確認済み(Confirmed)
- 潜在的(Potantial)
- 収集された情報(Information Gathered)



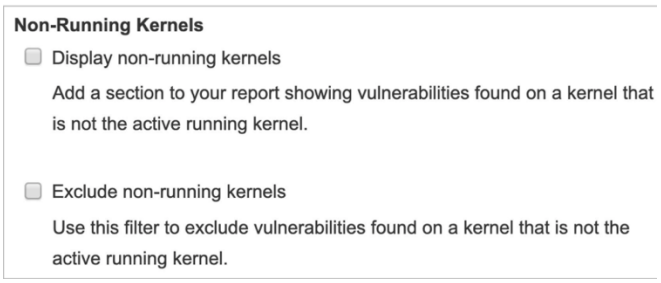
実行されていないカーネルフィルター

デフォルトでは、すべての Linux カーネル（実行中のカーネルと非実行中のカーネル）の脆弱性をレポートできます。表示オプションを選択すると、非実行中のカーネルの脆弱性をリストする新しいセクションがレポートに追加されます。除外オプションを選択すると、非実行中のカーネルの脆弱性が除外されます。

- レポートにセクションを追加して、Unix ベースの資産で実行されていないカーネルを表示します。

または

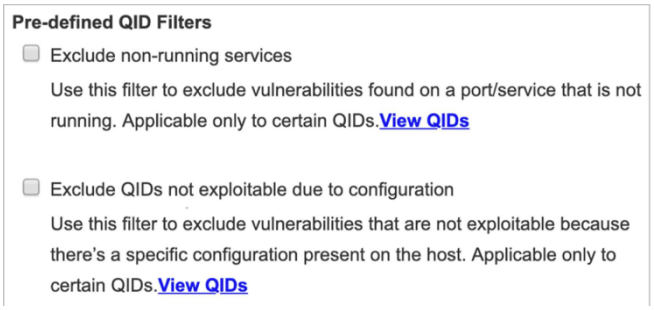
- 実行されていないカーネルをレポートから除外する



◉ VM API を使用してレポートを作成する場合の実行中のカーネルと実行されていないカーネルによるレポートの使用方法の詳細については、https://success.qualys.com/discussions/s/article/000006209 を参照してください。

定義済みの QID フィルター

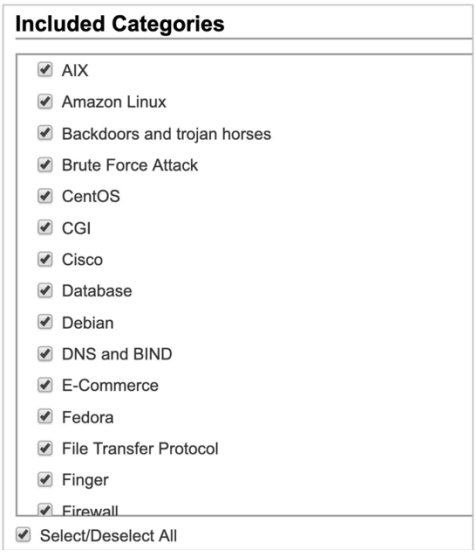
フィルターを選択して、レポートから特定の脆弱性（実行されていないポート/サービスで見つかった脆弱性や、ホストの設定により悪用できない脆弱性など）を除外します。これらのフィルターは特定の QID にのみ適用されます。



- 事前定義された QID フィルターは、特定の脆弱性リストにのみ適用されます。
- 「QID を表示」リンクをクリックすると、影響を受ける脆弱性が表示されます。

カテゴリーで絞り込む

ナレッジベースの各 QID にはカテゴリが割り当てられています。レポートに表示される QID をカテゴリで絞り込むことができます。例えば、TCP/IP カテゴリの脆弱性のみをレポートしたい場合などです。
Qualys では通常、すべてのカテゴリを選択することを推奨しています。これにより、一部の脆弱性がレポートに表示されない可能性が減ります。
カテゴリ内の脆弱性のリストを表示する場合は、ナレッジベースの検索機能を使用します。



- これらは Qualys 脆弱性ナレッジベースと同じカテゴリです。
- Qualys は、完全なカバレッジを確保するためにすべてのカテゴリを選択することを推奨しています。

スコアカードレポート

スコアカード レポートは、資産の全体的なセキュリティ状態を高レベルで提供します。

- **脆弱性スコアカードレポート**は、選択した資産グループまたはタグに関する最新の脆弱性ステータスをレポートします。
- **無視された脆弱性レポート**は、現在無視されている脆弱性を識別します。
- **最も蔓延している脆弱性レポート**は、検出されたインスタンス数が最も多い脆弱性を識別します。
- **最も脆弱なホストレポート**は、重大度レベル３， ４， ５の脆弱性の数が最も多いホストを識別します。
- **パッチレポート**は、必要なパッチとソフトウェアが不足しているホストを識別します。

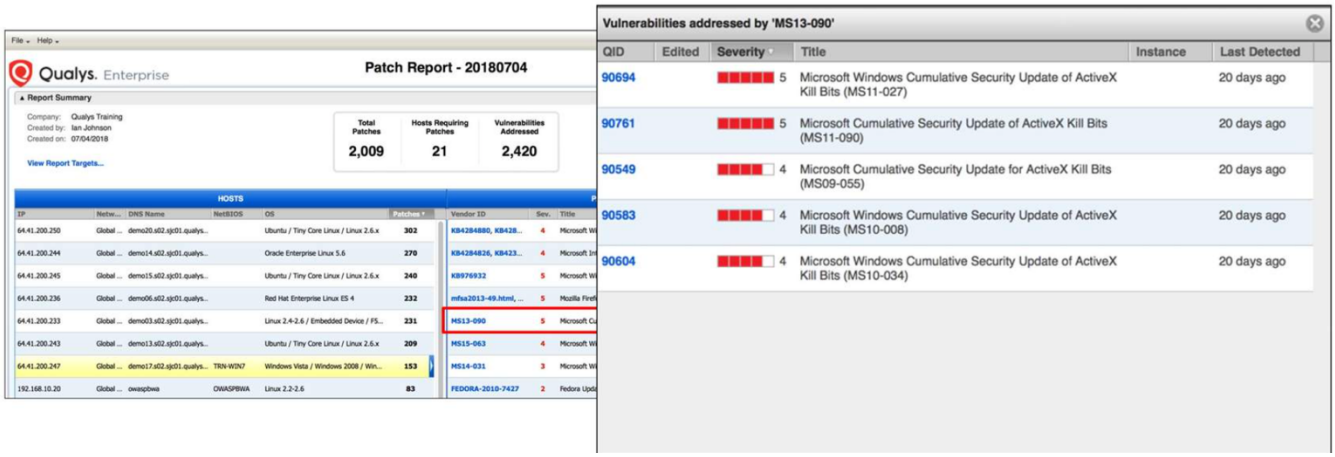
パッチレポート

1. パッチ レポートは、現在発見されている脆弱性を修正するためにインストールする必要があるパッチをリストするように設計されています。
2. パッチ レポートはオンライン レポートとして使用されることが多く、レポートを閲覧するユーザーはレポートの内容内を移動できます。
3. このオンライン形式では、レポートをダウンロードすることはできません。ただし、レポートの内容を PDF、XML、または CSV 形式でダウンロードするオプションがあります。
4. このレポートをオンライン形式で閲覧したい人は、サブスクリプションにアカウントを持っている必要があります。

置き換えを伴うパッチレポート

パッチレポートを使用すると、Qualys プラットフォームは自動的にパッチの置き換えを使用します。つまり、レポートに表示されるパッチは、QID の修正に必要な最新のパッチになります。そのパッチは他の QID の修正にも使用される可能性があり、その場合、それらの QID はすべてグループ化されます。

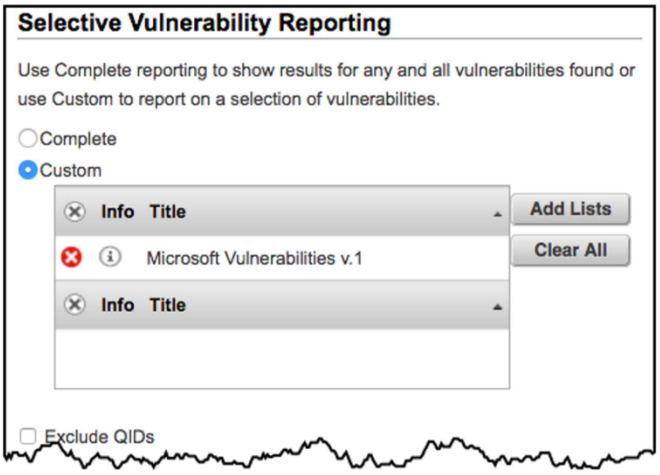
- パッチレポートには常に最新のパッチが表示されます。
- リストされているパッチは複数の QID を修正するために使用できる可能性があります。



選択的パッチレポート

デフォルトでは、利用可能なすべてのパッチがレポートに含まれます。
ただし、フィルターオプション「**選択的パッチレポート**」を使用すると、レポートに含めるパッチ QID と除外するパッチ QID を指定できます。「**完全**」を選択すると既知のパッチ QID がすべて表示されます。「**カスタム**」を選択すると特定のパッチ QID のみが表示されます。「**パッチ QID を除外**」を選択すると、特定のパッチ QID がレポートから除外されます。
例えば、Microsoft の脆弱性に関するパッチレポートを生成し、サービスパックの QID を除外したいとします。この場合、2 つの検索リストが必要

です。1 つ目の検索リストには、ベンダーが Microsoft である脆弱性が含まれます。2 つ目の検索リストには、脆弱性のタイトルに「Service Pack」が含まれるすべての脆弱性が含まれます。



「**選択的脆弱性レポート**」を使用し、「カスタム」を選択して、Microsoft 脆弱性検索リストを追加します。レポートには、ベンダーである Microsoft に関連する脆弱性のみが含まれます。次に、「**選択的パッチレポート**」を使用して、レポートから除外するパッチ QID を特定します。「**パッチ QID を除外**」を選択し、サービスパック検索リストを追加します。サービスパックに関連付けられた QID はレポートから除外されます。このテンプレートで生成されるパッチレポートには、サービスパックに関連付けられていないすべての Microsoft 脆弱性が含まれます

パッチの置き換え - 重要なポイント

- 「**置き換えられたパッチを除外**」機能を使用する場合、ホスト上でフラグが付けられた QID を分析するものであり、ホスト上でパッチがインストールされているかどうかや不足しているかどうかを分析するものではないことに注意してください。
- パッチの置き換えは、セキュリティ、経営幹部、監査人の評価、および環境内のリスク（脆弱性）に関する意思決定に影響を与えることを目的としたレポート データを生成するために**適用しない**でください。
- QID による置き換えによる抑制は、リスク（脆弱性）検出データに基づいて、技術修復担当者が手動で適用するパッチの適切なリストを特定・作成する場合にのみ適用可能であり、多少の潜在的価値をもたらす可能性があります。したがって、パッチの置き換えは慎重に検討してください。
- パッチの置き換えロジックは、オペレーティング システムと検出された QID に基づいてパッチのツリーをトラバースし、OS およびその他の基準を満たす最高のリードノードを見つけることによって実行されます。
- オプションプロファイルの脆弱性スキャン（完全な脆弱性スキャンではなくカスタムの脆弱性スキャン）から、または脅威保護 RTI や顧客検索リストを使用してレポートをフィルター処理することによって QID がフィルターされると、ツリー構造にギャップが生じ、置き換えロジックが壊れる可能性があります。
- **スコアカードのレポートとダッシュボード**は現在、パッチの置き換えをサポートしていないことに注意してください。

◉検索リストとパッチの置き換えを使用した場合のレポート結果の詳細については、
https: //qualysguard.qg2.apps.qualys.com/qwebhelp/fo_portal/search_lists/search_lists_exclude_superseded_pa tches.htm をご覧ください。
◉パッチの置き換えに関する詳細については、次のリンクを参照してください。
詳しい仕組み
QualysGuard は、置き換えられた Microsoft パッチをどのように処理しますか?

パッチの重大度を表示

ホスト上で検出されたパッチで修正可能なすべての QID の中で、最も高い重大度をレポートのパッチ重大度として表示したい場合は、「**最高重大度**」を選択します。例えば、パッチ MS09-015 が重大度レベル 3、4、5 の 3 つの QID を修正するとします。3 つの QID すべてがホスト上で検出された場合、パッチ重大度は 5 になります。一方、重大度 5 の QID がホスト上で検出されず、他の QID が検出された場合は、パッチ重大度は 4 になります。
QID 90492（重大度 3）、QID 90397（重大度 4）、QID 90342（重大度 5）。ホスト上で 3 つの QID がすべて検出された場合、パッチの重大度は 5 になります。ホスト上で QID 90342 が検出されず、他の QID が検出された場合、パッチの重大度は 4 になります。

	最高深刻度
パッチの重大度	MS09-015 – 重大度 5
検出された QID	QID 90492 – 重大度 3 QID 90397 – 重大度 4 QID 90342 – 重大度 5

割り当てられた重大度の例をご覧ください。パッチレポートに示されているように、このパッチには重大度 3 が割り当てられています。ただし、このパッチで対処されている脆弱性の重大度はそれぞれ異なり、この例では 5 と 4 です。

レポートの展開

レポートの展開とは、次のことを意味します。

- どのような種類のレポートを実行する必要がありますか?

大量のスキャンデータとクラウドエージェントデータを精査する必要があります。優先順位付けと修復を効果的に行い、社内の関係者に適切な概要データを提供するには、どのようなレポートを実行する必要がありますか？

- 誰がそれを手に入れるのでしょうか?

組織内のどのユーザーが業務を効果的に遂行するためにレポートを受け取る必要があるのでしょうか？また、どのように説明責任を果たせるのでしょうか？脆弱性管理プログラムが機能していることを確認するために高レベルのレポートを参照する必要があるユーザーは誰でしょうか？また、修復の推進や検証に役立つレポートを必要とするユーザーは誰でしょうか？

- いつ受け取れる予定ですか？

これは、レポートをスケジュールし、脆弱性管理プロセスを可能な限り自動化するプロセスです。

レポートの配布

レポートを配布する方法は複数あります。

Qualys ユーザーへのレポートの配布 - オプション 1

- マネージャーは、必要な資産をユーザー（リーダー/スキャナーの役割のユーザー）に割り当てます。

- ユーザーはテンプレートを使用してレポートを作成またはスケジュールします

Qualys ユーザーへのレポートの配布 - オプション 2

- マネージャー ユーザーは、レポートの生成に使用するレポート テンプレートを作成します。
- マネージャーユーザーは、ユーザーをレポートテンプレートに割り当てます。
- このテンプレートを使用してレポートを実行すると、テンプレートに割り当てられたユーザーは、テンプレートに含まれるアセットへのアクセス権がない場合でもレポートを表示できるようになります。

必要なすべてのユーザー（Qualys ユーザーと非 Qualys ユーザー）にレポートを配布する

- マネージャーユーザーがレポートテンプレートを作成します。
- マネージャユーザーは、Qualys アカウントを持つユーザーとアカウントを持たない人のメールアドレスを含む配布グループを作成します。
- マネージャーユーザーはレポートをスケジュールし、配布グループを含めます。
- スケジュールされた時間にレポートが実行されると、配布グループ内のユーザーはレポートにアクセスするための添付ファイルまたはリンク（設定によって異なります）を受け取ります。

スケジュールされたレポート

マッピングやスキャンと同様に、レポートも定期的に、指定した時間に自動実行するようにスケジュール設定できます。また、レポートが完成し、表示可能になった際に、選択した配布グループに通知するオプションを設定することもできます。

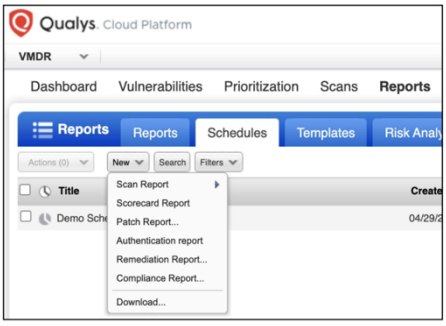
レポートをスケジュールする:

スケジュール設定できるレポートの種類は複数あります。テンプレートベースのスキャンレポート（ホストベースの検出結果に設定）、スコアカードレポート、パッチレポート、テンプレートベースのコンプライアンスレポート、修復レポートをスケジュール設定できます。

新しいレポートスケジュールを作成するには、「レポート」>「スケジュール」に移動し、「新規」メニューから必要なレポートの種類を選択します。以下の例では、テンプレートベースの新しいスキャンレポートをスケジュールしています。

次のレポートタイプをスケジュールできます。

- テンプレートベースのスキャンレポート（ホストベースの検出を使用）
- スコアカードレポート
- パッチレポート
- 認証レポート
- 修復レポート



スケジュールレポートの設定

スケジュールされたレポートを構成する場合、レポートを配布するための 4 つのオプションがあります。

- **添付ファイルまたはリンク:** このオプションを使用すると、レポートのサイズが 5 MB 未満の場合、レポートは添付ファイルとして送信され、それ以外の場合はレポート リンクが送信されます。
- **添付ファイルのみ:**このオプションを選択すると、レポートのサイズが 5 MB 未満の場合、レポートは添付ファイルとして送信されます。それ以外の場合、レポートは送信されません。
- **リンクのみ:**このオプションを選択すると、レポート リンクが常に送信されます。
- **レポートを送信しない：**このオプションを選択すると、レポートは添付ファイルまたはリンクとして送信されません。ユーザーはレポートを閲覧するために Qualys コンソールにログインする必要があります。

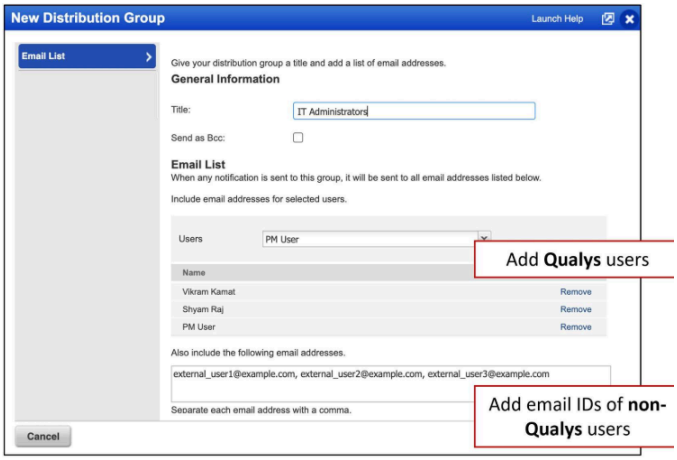
注記：
レポートがリンクとして送信された場合、受信者はできるだけ早くリンクからレポートをダウンロードする必要があります。レポートは 7 日後、またはそれ以前に（ユーザーの共有制限が割り当てられた最大サイズに達した場合）レポート共有から削除されるためです。

配布グループ

次のようないくつかの電子メール通知の配布グループを選択できます。

- スキャン通知
- 通知を報告し、
- 脆弱性通知

たとえば、スキャンまたはレポートが完了したときにグループに通知できます。
VM アプリケーションの**[ユーザー] -> [配布グループ]**タブで**配布グループ**を作成できます。



サブスクリプション内のユーザーの電子メール アドレスを含めることも (リストからユーザーを選択するだけ)、サブスクリプション外のユーザーの電子メール アドレスをテキスト フィールドに入力して含めることもできます。

サブスクリプションの設定

デフォルトでは、Qualys ユーザーごとにレポート保存容量が 200 MB 割り当てられます。マネージャーユーザーは、この容量をユーザーごとに最大 500 MB まで増やすことができます。

PDF レポートを暗号化するには、[レポート] > [設定] > [レポート共有] で安全な PDF 配布設定を有効にします。

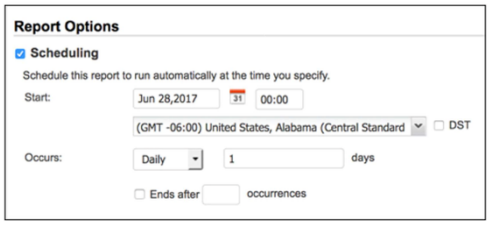
- Report Share はレポートを保存し共有するための集中的な場所です。
- サブスクリプションを有効にすると、管理者は各ユーザーが保存できるレポートデータの最大量を指定します。
- 管理者はレポートの安全な PDF 配布を有効にするオプションがあります。

スケジュールとレポート通知

新しいレポートスケジュールを作成するには、**「レポート」>「スケジュール」に移動し、「新規」**メニューから必要なレポートの種類を選択します。すると、「**新規スキャンレポート**」ページが表示されます。

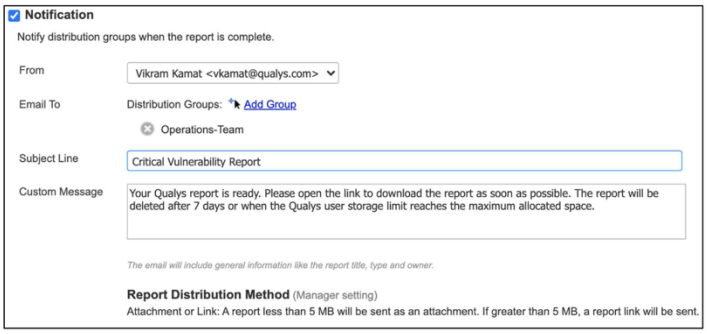
スケジュール

スケジュールレポートの開始日時と、レポートの実行頻度を定義します。例えば、毎日、毎週、毎月、指定した曜日にレポートを実行するようにスケジュールを設定できます。



報告通知

レポートが完成し、閲覧可能になった際に通知する相手を定義します。レポート通知は、選択した配信グループに登録されているすべてのメールアドレス（Qualys アカウントを持つユーザーと持たないユーザーの両方）に送信されます。メールの属性（送信者（お客様または Qualys サポート）、件名、本文）をカスタマイズできます。生成されたレポートが 5MB 未満の場合は、生成された形式でメールの添付ファイルとして送信されます。5MB を超える場合は、添付ファイルではなく、メール内にリンクが提供されます。レポートをリンクとして送信した場合、受信者はできるだけ早くリンクからレポートをダウンロードする必要があります。レポートは 7 日後、またはそれ以前に（ユーザーの共有制限が割り当てられた最大サイズに達した場合）レポート共有から削除されます。そのため、レポート受信者が理解できるよう、カスタムメッセージ領域にこのような情報を追加することをお勧めします。スケジュールされたレポートはスケジュール リストに表示され、レポートはスケジュールされた時間に実行されます。



レポートを実行するのに最適な時期はいつですか?

レポート機能は、サブスクリプションで既に利用可能なデータに基づいて、技術インフラストラクチャのリスク状況を包括的かつ集中的に把握することを目的としています。これにより、チームは検出データの精度をデータに基づく実用的な意思決定へと変換できます。アカウント内のスキャンデータが変更されているときにレポートを実行すると、レポートに一貫性がなくなる可能性があります。そのため、環境内でスキャンが実行されていないときにレポートの実行やスケジュール設定を検討してください。VM アプリケーションの**「スキャン」>「スケジュール」**タブでスキャンスケジュールを確認し、環境内で通常スキャンが実行される時間を特定できます。
エージェントホストに関するレポートを作成する際には、Cloud Agent のスキャンアクティビティも考慮する必要があります。すべての Cloud Agent が同時に Qualys クラウドプラットフォームにスキャンデータをアップロードするわけではないため、この点は少し複雑です。クエリ（lastFullScan）やダッシュボードを使用して Cloud Agent のアクティビティを追跡し、環境内のエージェントホストに関するレポートを実行する最適なタイミングを判断してください。

- スキャンデータが変更されていない場合はレポートを実行することを検討してください
- スキャンスケジュールを使用して、環境内で通常いつスキャンが実行されるかを識別します。
- スケジュールの時間を決める際には、クラウドエージェントのスキャンアクティビティも考慮してください。

例外管理

このレッスンでは、脆弱性例外の管理プロセスの概要を説明します。

例外の必要性

レポート作成の文脈において、**例外は脆弱性カウントから情報を抑制（非表示）するために使用**されます。Qualys の脆弱性フラグが **Closed/Ignored** になっている間も、検出情報はサブスクリプションデータベースに残っていることに注意することが重要です。

1. 修復プログラムは、利用可能なリソースと組織が直面する特定のリスクに応じて、組織ごとに異なります。
2. 潜在的な脅威を特定し評価することは重要なステップですが、最も時間のかかるステップは脆弱性への対応です。ここで、脆弱性の修復と、関連するリスクを受け入れて脆弱性を無視すること（例外管理）のどちらが重要になります。どちらも脆弱性への対応における異なるアプローチであり、対処する脆弱性の種類に応じてそれぞれにメリットがあります。
3. 脆弱性によってもたらされるリスクを受け入れることは、リスク軽減戦略とは言えません。リスクを受け入れても、その効果は低下しないからです。しかしながら、リスクの受け入れは脆弱性管理において正当な選択肢の一つです。
4. 脆弱性に対処するコストがメリットを上回る場合や、セキュリティ対応を実施するためのリソースが限られている場合、ほとんどの組織は、リスクを軽減するために時間やリソースを費やすのではなく、リスクを受け入れることを選択します。

例外処理が適格なシナリオ

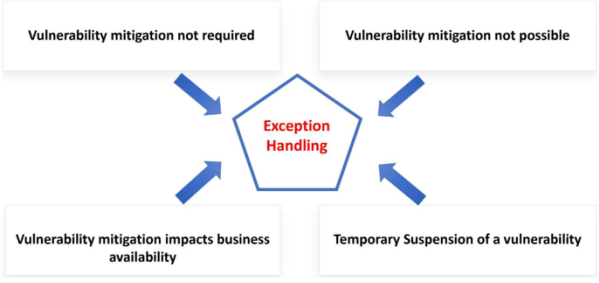
脆弱性の修復または軽減が不可能または実用的ではない可能性があるシナリオをいくつか示します。

まず、**すべての脆弱性を修正する必要はありません。**例えば、Adobe Flash Player に脆弱性が特定されたとしても、社内のすべての Web ブラウザとアプリケーションで Flash Player の使用が既に無効になっている場合は、対策を講じる必要はありません。

場合によっては、問題の脆弱性に対するパッチがまだ利用できないなど、技術的な問題により修復措置を講じることができないことがあります。

場合によっては、組織から抵抗を受けることもあります。これは、顧客対応システムに脆弱性があり、脆弱性を修正するために必要なダウンタイムを回避したい場合によく発生します。

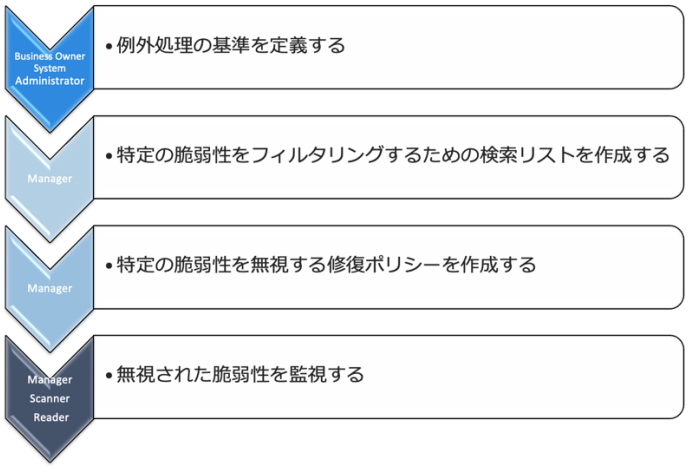
最後に、**様々な理由により、脆弱性を一時的にクローズする必要がある場合**があります。例えば、脆弱性が存在しないにもかかわらず、誤検知が発生しているケースの調査が進行中の場合などです。このような場合、決定的なデータが得られるまで、このような脆弱性を一時的にクローズすることが考えられます。また、パッチ適用チームが本番環境への展開前に、テスト環境または UAT 環境でパッチをテストする時間が必要な場合も考えられます。このような脆弱性は、後でパッチが適用される



ため、一時的にクローズする必要があります。あるいは、組織が変更凍結を課し、特定の脆弱性を一時的にクローズし、修復作業を後日延期する必要がある場合もあります。

例外を自動的に管理する

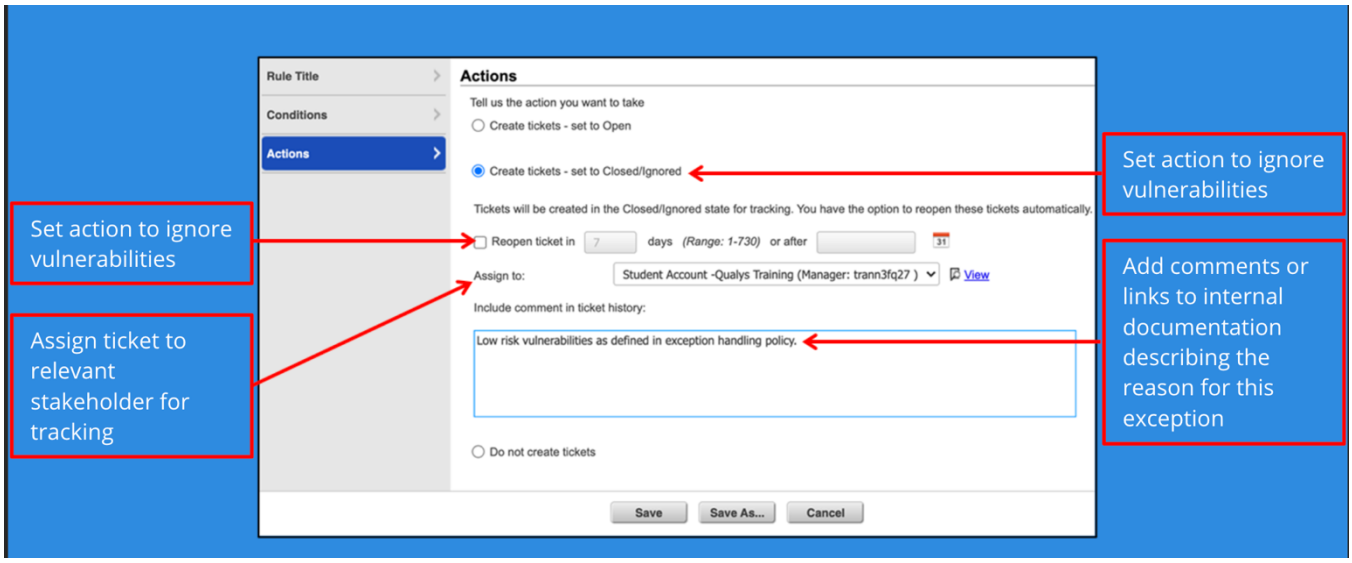
以下の画像は、**脆弱性管理で修復ポリシーを使用して例外処理を設定する手順**を示しています。
例外を作成および承認する際には、例外がデリケートなビジネス上の問題に対処するものであることを理解することが重要です。例外が承認されるということは、脆弱性を修正しなかった場合の結果を認識し、同意することになるので、リスクを受け入れることを意味します。したがって、**これらの例外がどのように評価され、どのように承認されるかが重要**です。したがって、例外を管理するための明確かつ明確に定義されたプロセスを用意することが推奨されます。



1. 事業責任者や資産所有者、システム管理者は、**例外事項の提起と承認の基準**を設定する必要があります。また、確立されたプロセスからの逸脱は、適切な承認および変更管理プロセスを経る必要があります。
2. 次のステップは、例**外処理の対象となる脆弱性を特定するための基準を適用**することです。検索リスト（静的および動的）を使用して、例外処理基準に一致する特定の脆弱性をフィルタリングできます。Qualys Manager ユーザーアカウントには、検索リストを設定する権限があります。
3. **修復ポリシー**は、検出された脆弱性を修復担当者に割り当て、軽減措置を講じるために一般的に使用されます。ただし、これらのポリシーは、例外処理基準に従って対処する予定のない脆弱性を自動的に無視し、リスクを受け入れるためにも使用できます。また、ホストベースの検出結果やアセット検索結果から得られるホスト情報に基づくスキャンレポート（HTML 形式）を使用して、脆弱性を手動で無視することもできます。
4. 最後に、例外処理プロセスが期待どおりに機能していることを確認するために、**無視された脆弱性を追跡・監視する必要があります**。スキャンレポートテンプレートのフィルターを使用することで、アカウント内のすべての無視された脆弱性をレポートできます。

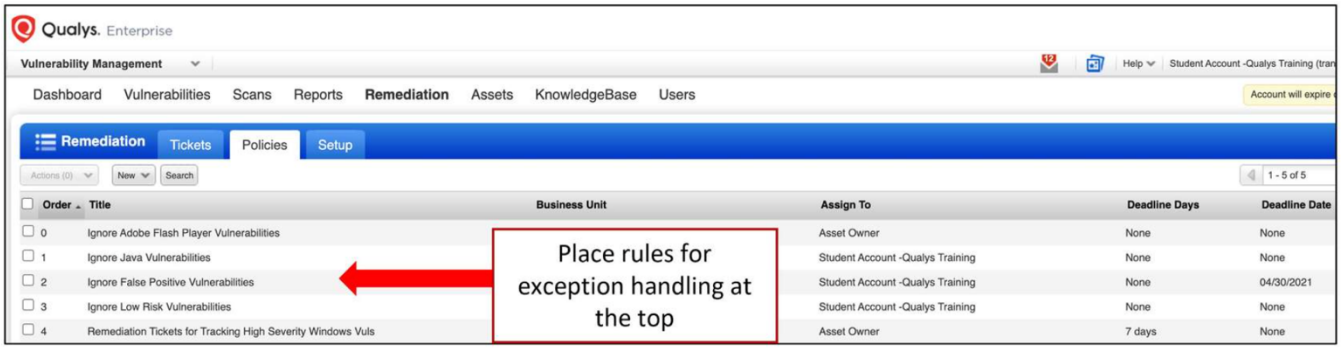
修復ポリシーを構成する

トレーニングビデオでは、脆弱性を無視する修復ポリシーを構成する方法について説明します。



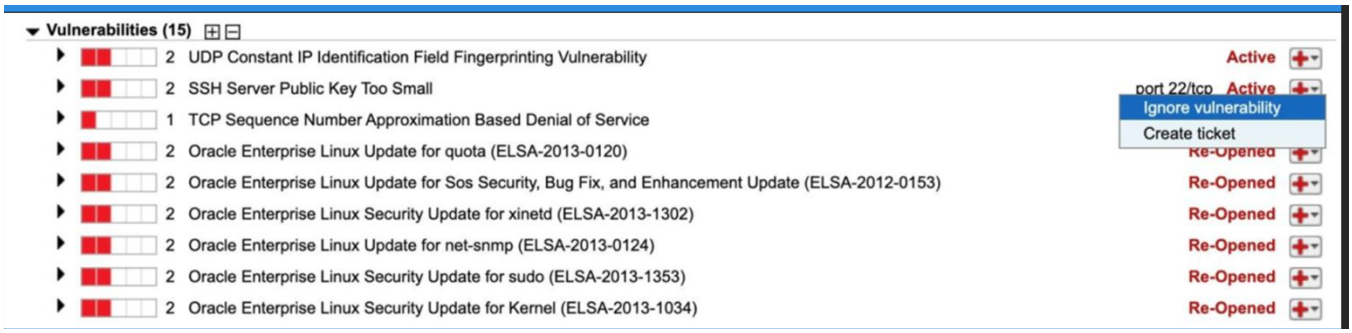
脆弱性を無視するルールを優先する

- 修復ポリシールールは、リストされている順序でスキャン結果に適用されます。
- 脆弱性にルールが適用されると、条件が脆弱性と一致しても、後続のルールは再度適用されません。
- 例外処理のためのルールを先頭に配置することをお勧めします



例外を手動で管理する

トレーニングビデオでは、脆弱性を手動で無視する方法を説明しています。

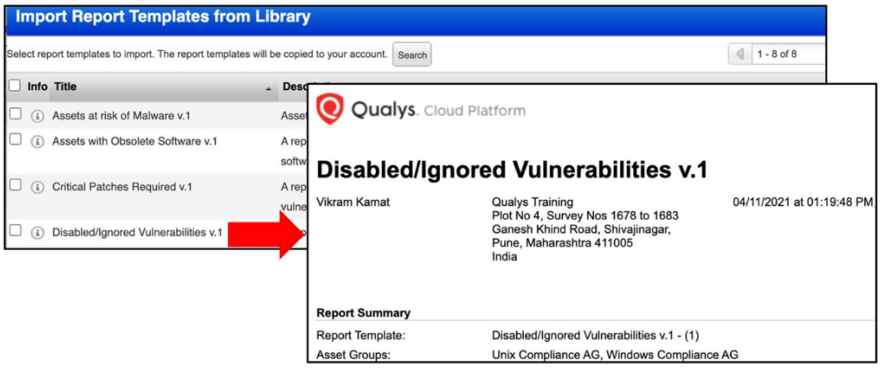


無視された脆弱性を監視する

複数の方法を使用して、**永続的に無視された脆弱性や指定された期間延期された脆弱性を追跡**できます。

○Disabled/Ignored 脆弱性 v.1 テンプレート

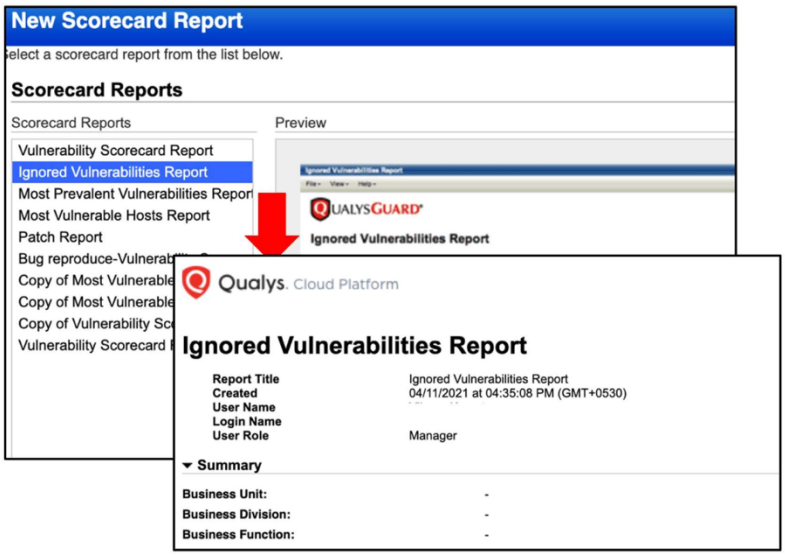
無効化および無視された脆弱性をフィルターするように構成された、テンプレート ライブラリ**の無効化/無視された脆弱性 v.1 テンプレート**を使用することもできます。



○Ignored 脆弱性スコアカードレポート

あるいは、スコアカード レポートの一部として利用できる **Ignored** 脆弱性レポートを使用して、このレポートを生成することもできます。

このレポートでは、現在無視されている脆弱性が特定されます。対象となる各アセットグループには、グループ内のホストで無視されている脆弱性がリストされます。レポートには、ホストの詳細、脆弱性の詳細、および修復チケットの詳細が表示されます。



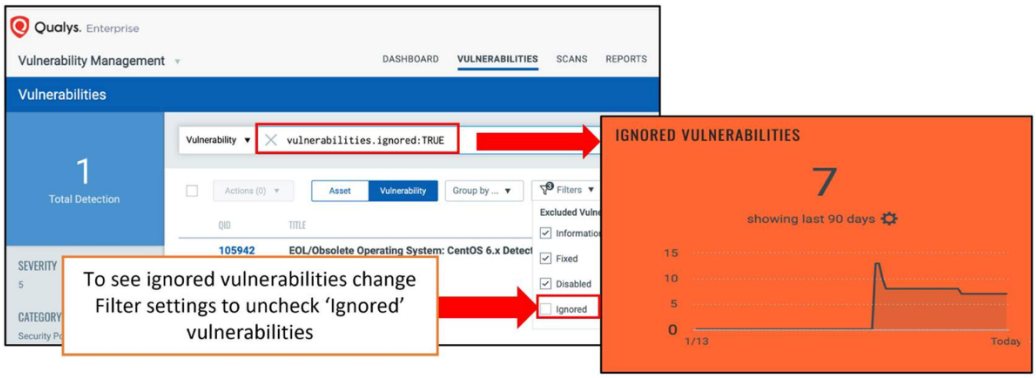
○検索クエリとウィジェット

最後に、次の QQL クエリを使用して、検索結果で無視された脆弱性を一覧表示できます。

Vulnerabilities.ignored: TRUE

無視された脆弱性は、デフォルトでは検索クエリの結果に表示されません。これらの脆弱性を表示するには、フィルター設定を変更し、「無視」された脆弱性のチェックを外してください。

上記の検索クエリを使用して、無視された脆弱性を追跡するためのダッシュボード ウィジェットを作成し、これらの脆弱性を追跡するための傾向分析を有効にすることができます。



レポートの使用例

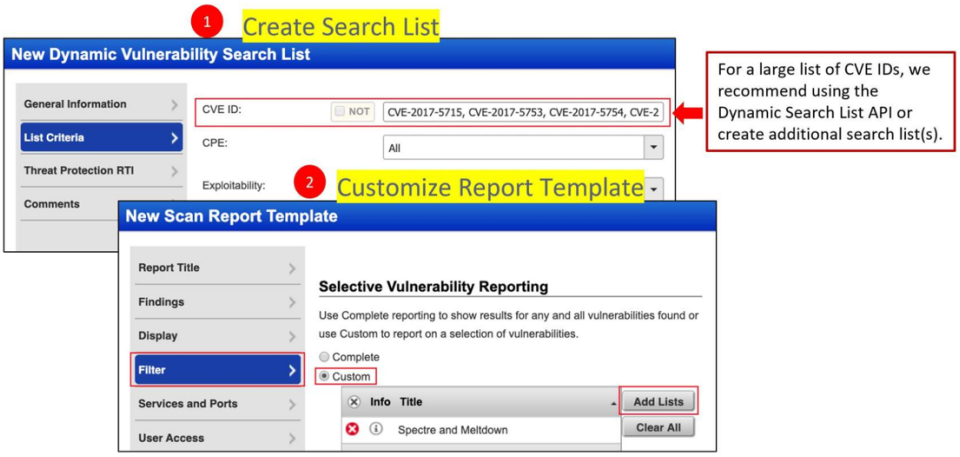
このレッスンでは、いくつかの実用的なユースケースにおける脆弱性報告の対応方法について説明します。具体的には、主要な脆弱性に関連する QID の特定、必要な検索リストの構築、検索クエリとダッシュボードウィジェットを使用したパッチ火曜日リリースの更新管理のライフサイクルなどについて説明します。

報告ユースケース - 重大な脆弱性のリリース

- 場合によっては、**組織は特定の重大度の高い脆弱性や脅威の高い脆弱性に直ちに対処する必要がある**。
- これらのタイプの脆弱性は「**後回しにせず、今すぐ対処する**」カテゴリーに分類されます。
- 例: Spectre および Meltdown、Patch Tuesday リリースの一部として公開された脆弱性など。

Spectre と Meltdown の脆弱性に関する報告

最初のステップは脆弱性を検出することです。通常の VM スキャンでは、すべての QID（オプションプロファイルのデフォルト設定）が対象となります。**レポートに必要な QID のみを含む検索リストを作成できます。**例：Spectre および Meltdown の脆弱性。検索リストを作成したら、**レポート内で脆弱性フィルターとして使用できます。**生成されるレポートには、検索リストの設定に一致する QID のみが含まれます。これを行うには、レポートテンプレートを編集し、検索リストを含めます。



◎UI に入力できる文字数には制限があることにご注意ください。CVE ID の大規模なリストが必要な場合は、動的検索リスト API のご利用をお勧めします。詳細については、VM API ユーザーガイドをご覧ください。また、追加の検索リストを作成することもできます。スキャン用のオプションプロファイル、またはレポート用のレポートテンプレートには、複数の検索リストを含めることができます。

レポートのユースケース - パッチ火曜日リリース

Patch Tuesday （ Update Tuesday とも呼ばれる）は、Microsoft、Adobe、Oracle などの企業が自社ソフトウェア製品のパッチを定期的にリリースする日を指す非公式用語です。業界では広くこの呼び方で呼ばれています。Microsoft は 2003 年 10 月に Patch Tuesday を公式化しました。北米では、Patch Tuesday は毎月第 2 火曜日（場合によっては第 4 火曜日）に実施されます。マイナーアップデートは Patch Tuesday 以外にもリリースされます。

Qualys アドバイザリの概要:
Qualys 脆弱性 R&D ラボは、毎月の Patch Tuesday リリースの一環として Microsoft が発表するセキュリティ情報で修正された脆弱性から組織を保護するために、Qualys クラウド プラットフォームで新しい脆弱性チェックをリリースします。

◎これらの脆弱性の詳細は、Qualys セキュリティアラートの一部として定期的に公開されており、
https://www.qualys.com/research/security-alerts/で確認できます。

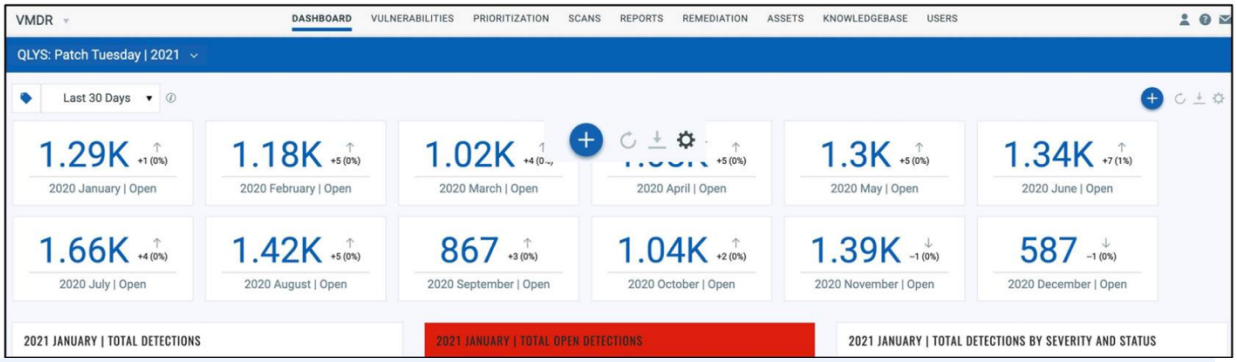
パッチ火曜日の脆弱性を発見

Qualys VM/VMDR は、ナレッジベース（KB）の継続的な更新を利用して、Patch Tuesday で新たに発見された脆弱性を自動的に検出します。**Qualys のお客様は、QQL クエリで対応する QID を使用することで、Qualys サブスクリプション内の Patch Tuesday やその他の新たな脆弱性について、ネットワークを監査できます。**

Using QQL searches

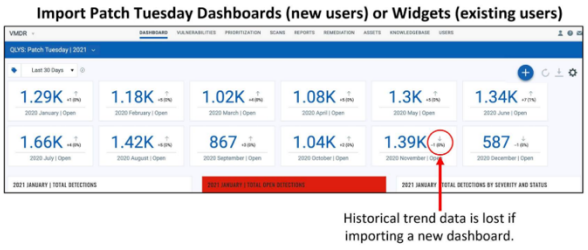
Qualys は、**各パッチ火曜日リリース用のダッシュボードとウィジェットも提供しています。**このダッシュボードで使用されるクエリ文字列は、毎月の Qualys セキュリティアラート投稿に基づいて作成されています。これらのアラートには、指定された月次パッチ火曜日サイクルで Microsoft および Adobe 向けにリリースされた QID が含まれています。今後の参照のために、Qualys セキュリティアラートをブックマークすることを強くお勧めします。

Import Patch Tuesday Dashboards or Widgets



◎これらのダッシュボードとウィジェットは、Qualys コミュニティで検索できます:
https://community.qualys.com（新しいタブで開きます）

◎最新の Patch Tuesday ダッシュボードとウィジェットは、このリンクからダウンロードできます:
https://success.qualys.com/discussions/s/article/000006505



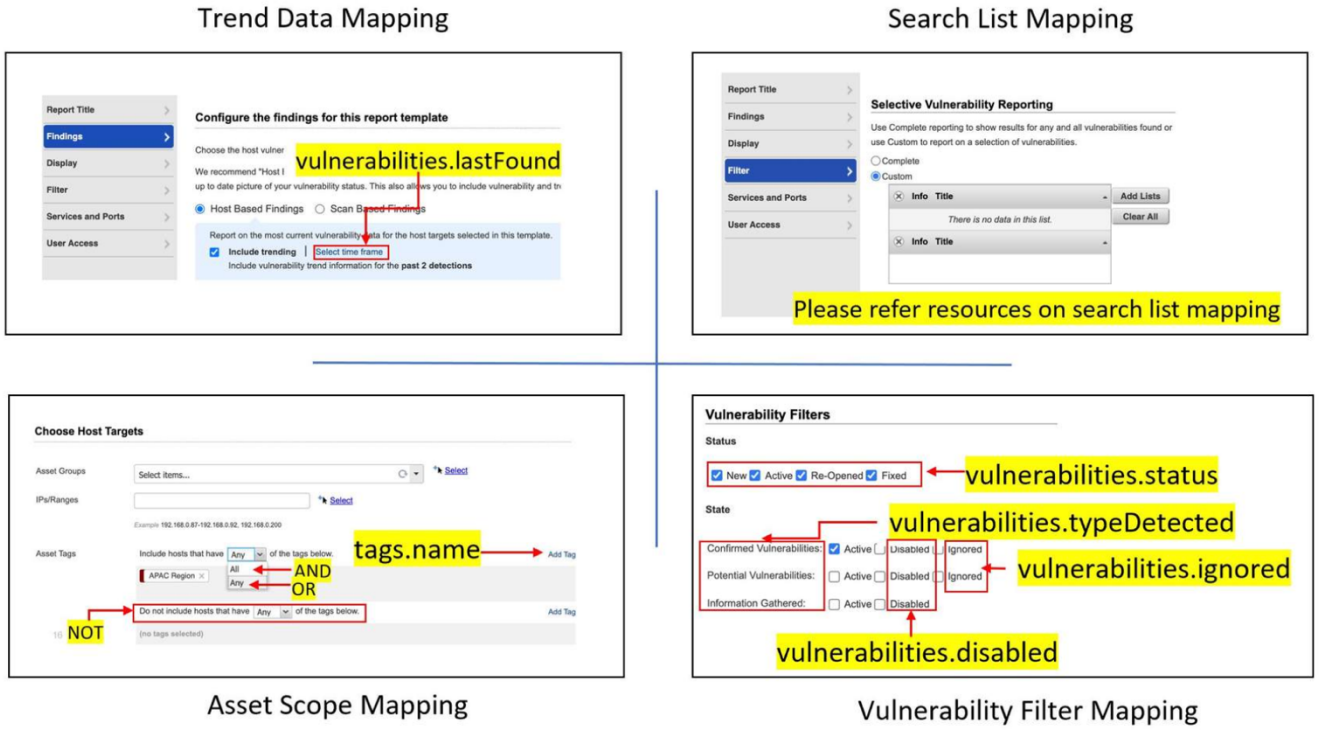
- まったく新しいダッシュボード ユーザーの場合は、**QLYS_Patch_Tuesday_2021-xx-Month_Vmdashboard** という名前のファイルから (単一の JSON を含む)ダウンロードしてインポートしてください。
- 定期的な月次更新ユーザーの場合は、2021-xx-Month_UDWidget_JSON という名前のファイルから (複数のウィジェット JSON ファイルが含まれています)ダウンロードしてインポートしてください。

- JSON インポートの後に「**履歴データ収集を有効にする**」を有効にする必要があります。
- ダッシュボード ウィジェットの履歴データ収集を有効にする方法については、こちらをご覧ください。

注意:アカウントに Patch Tuesday (PT) ダッシュボードがすでに設定されている場合は、新しいダッシュボードではなく、Qualys コミュニティから新しい PT リリースのウィジェットをインポートすることを検討してください。そうしないと、アカウントの既存のダッシュボードの傾向データが失われます。

レポートテンプレートからダッシュボードウィジェットを作成する

データの視覚化を向上させるために、レポートテンプレートにマッピングされたダッシュボードウィジェットを作成することをお勧めします。レポートテンプレートの設定またはフィールドが VM クエリトークンにどのようにマッピングされているかを理解することが重要です。そうしないと、バッチレポートの件数がダッシュボードの件数と一致しなくなります。以下のスクリーンショットは、VM クエリトークンをスキャンレポートテンプレートの検出結果/検出日、アセット選択フィールド、および脆弱性フィルター設定にマッピングした画像を示しています。



詳細については、次のドキュメントを参照してください。

VM ダッシュボード: スキャンレポートテンプレートの検出結果/検出日と資産選択フィールドを VM ダッシュボードトークンにマッピング

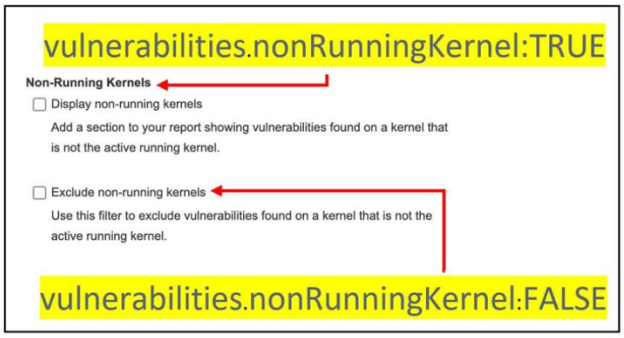
https://success.qualys.com/discussions/s/article/000005934（新しいタブで開きます）

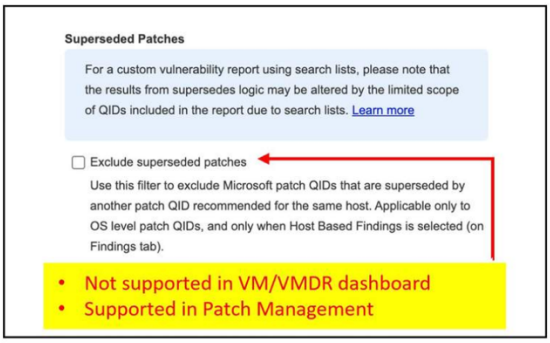
VM ダッシュボード: VM 検索リスト条件と VM ダッシュボード トークンのマッピング v2

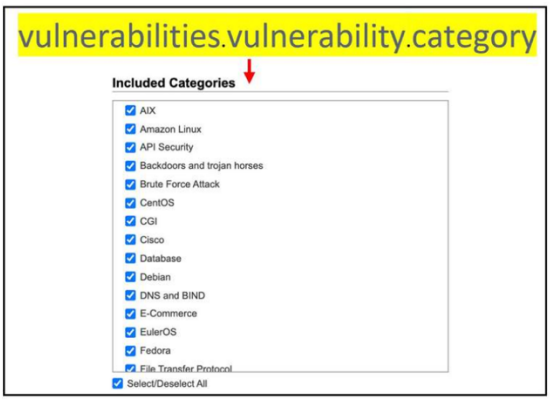
https://success.qualys.com/discussions/s/article/000005978（新しいタブで開きます）

VM ダッシュボード: スキャンレポートテンプレート/フィルターと VM ダッシュボードトークンのマッピング

https://success.qualys.com/discussions/s/article/000005938





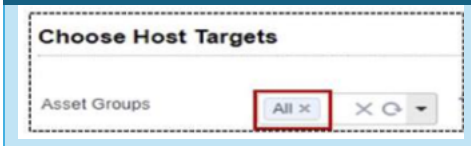


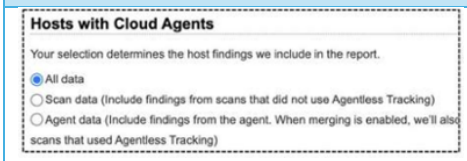
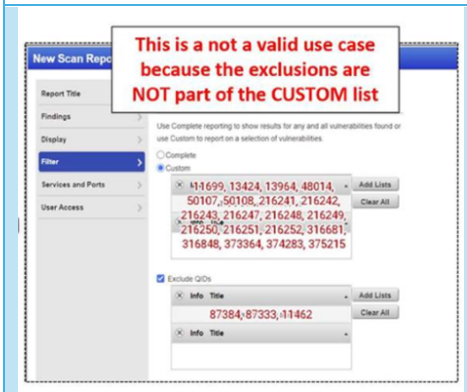
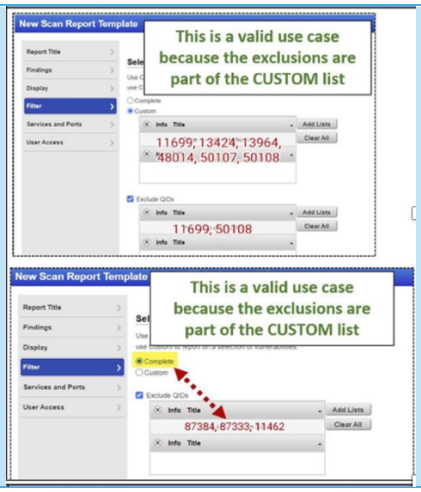
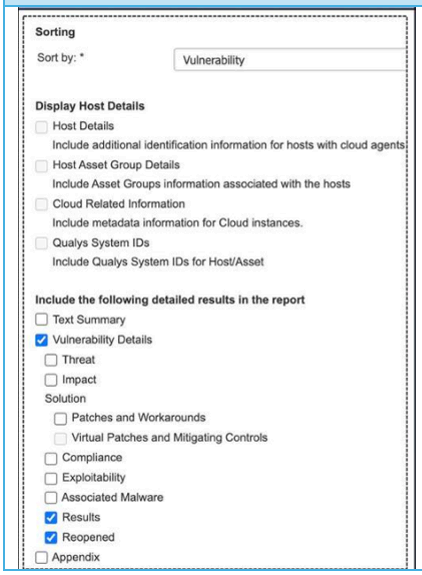
◉ パッチの置き換えは現在、VM/VMDR ダッシュボードではサポートされていません。ただし、パッチ管理アプリケーションではサポートされています。

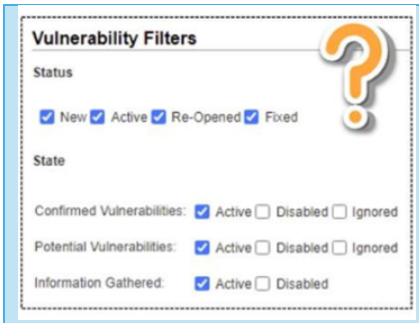
レポートの生成に時間がかかりすぎる、またはエラーが発生する

レポートの生成に時間がかかりすぎたり、エラーが発生したりする状況が発生することがあります。これらの状況は通常、**検出期間が長すぎる、資産スコープが大きすぎる、またはその他の設定が長すぎることが原因**で発生します。これらの設定が、検出期間と資産スコープの広さに重なると、レポートデータの処理に時間がかかり、エラーが発生する可能性があります。このユースケースでは、VM レポートテンプレートのいくつかの領域を分析し、レポートを効率的、効果的、かつ確実に実行するために微調整できる点について説明します。

各レポートテンプレートのセクションでは、正しく設定されていない場合、レポート生成に長時間かかったりエラーが発生したりする可能性のある設定について概説しています。また、各セクションでは、これらの問題を防ぐための推奨事項も提供しています。

テンプレートセクション	説明	推奨事項とリソース
	レポートの受信者が 1 人だけであれば、すべてのスコープが適切である可能性がありますが、これは一般的ではありません。	- レポートツールボックス：レポートのベストプラクティスに関する FAQ - 受信者に合わせてレポート内の資産範囲を再設定する

	アセットスコープが多すぎると、レポート生成中にタイムアウトやエラーが発生する可能性があります。	
	必要なものだけを含めてください。データの選択を微調整することで、効率的、効果的、そして確実に実行されるテンプレートを作成できます。 上記の設定に加えて「すべてのデータ」を選択すると、レポート生成中にタイムアウトやエラーが発生する可能性があります。	アプライアンスベースのスキャンとクラウドエージェントのみを実行しているサブスクリプションでは、**すべてのデータを**選択する必要があります。それ以外の場合は、次の条件に該当します。 - アプライアンスベースのスキャンのみを実行している場合は、「**スキャンデータ**」を選択します。 - クラウドエージェントスキャンのみを実行している場合は、「**エージェントデータ**」を選択します。
 **除外はカスタム リストの一部ではないため、これは有効な使用例ではありません。**	カスタムの包含 QID 検索リストには、除外 QID リストの QID は含まれません。	
	必要なものだけを含めてください。データの選択を微調整することで、効率的、効果的、そして成功につながるテンプレートを作成してください。 このセクションの選択は適切であり、上記の説明と一致しています。	レポートの受信者に連絡し、ホスト別にレポートを並べ替える方法が適切かどうかを確認してください。  **参考情報** - Windows 管理者は OS 別に並べ替えることを好む傾向があります。 - データベースチームは脆弱性別に並べ替えることを好む傾向があります。 - ネットワークチームは、特に IP アドレス範囲でアセットグループを分類している場合、アセットグループ別に並べ替えることを好む傾向があります。

	必要なものだけを含めます。 データの選択を微調整して、効率的、効果的、そして成功裏に実行されるテンプレートを作成します。	- このセクションの選択がレポートの範囲と一致していることを確認してください。あなたのポリシーが“Confirmed, Severity 3,4, &5 を確認した場合、チェックされたボックスが多すぎます。 - トレンドレポートでは、収集された情報がレポートデータの選択基準に含まれていることは稀です。 -すべてのオープン項目（New、Active、Reopen など）に対して一連のレポートを実行し、クローズされた項目（修正済みなど）に対して個別のレポートを実行することを検討してください。 -レポートを「オープン」と「クローズ」に分割すると、受信者にとってレポートが小さくなり、理解しやすくなり、エラー状態の変化が減ります。

コースサマリ

このコースでは、Qualys レポート戦略とベストプラクティス（RSBP）について学びました。

レポートは脆弱性管理プログラムにおいて非常に重要な要素です。レポートのベストプラクティスとコア目標を常に考慮することで、真の成果をもたらすレポートを作成できます。

レポートを標準とポリシーに準拠させる

レポートを組織のセキュリティ標準、ポリシー、ガイドラインに準拠させましょう。まずは、何を達成したいのか、なぜそのレポートを作成する必要があるのか、そして誰を対象に作成するのかを明確に定義することから始めましょう。これにより、成果物が明確になります。

関係者との調整と協力

レポートは協力して作成しましょう。ステークホルダーによってニーズは異なります。レポートを誰が読むのかを念頭に置き、何に焦点を当てるべきかを明確にしましょう。レポートやダッシュボードの改善・強化にあたっては、緊密なチームとして協力し、全員のアイデアや視点を取り入れましょう。そうすることで、成果物のターゲットオーディエンスを明確に把握できます。

資産の追跡と分類

IT インフラストラクチャを定期的に評価することで、資産のライフサイクル全体にわたって追跡・分類できます。これにより、非アクティブな資産、廃止された資産、再利用された資産をプロアクティブに特定し、Qualys アカウントから古いデータを削除する手順を踏むことができます。

データの衛生状態を維持する

古くなった脆弱性データを削除するため、廃止された資産を特定し、パージする計画を策定してください。Qualys の適切な資産管理オプションを使用して、可能な限り古くなったデータの削除を自動化してください。

適切なレポートツールを使用する

簡単な質問への回答を探している場合は、クエリをご利用ください。クエリを視覚的に表現したい場合は、ウィジェットをご利用ください。ダッシュボードは複数のウィジェットで構成されています。共通のテーマを持つウィジェットは、単一のダッシュボードに配置されます。
詳細な脆弱性情報を探している場合や、パッチ管理プログラムを監査したい場合は、レポートテンプレートをご利用ください。
Qualys UI Reporting は、サブスクリプションからすべての脆弱性をエクスポートしたり、大規模なデータをエクスポートしたりすることを目的としていないことに注意してください。大規模なデータのエクスポートには、Qualys API の使用をご検討ください。

以上