VMDR OT

スタートガイド

2023 年 1 月 24 日

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

目次

このガイドについて

Qualys VMDR OT に関心をお寄せいただきありがとうございます。Qualys VMDR OT は、制御、監視、サイト運用など、すべての産業用ネットワーク層にわたる重要なインフラストラクチャの包括的な可視性と脆弱性管理を提供します。

Qualys について

Qualys, Inc.(NASDAQ:QLYS)は、クラウドベースのセキュリティおよびコンプライアンスソリューションのパイオニアであり、リーディングプロバイダーです。Qualys Cloud Platform とその統合アプリは、重要なセキュリティインテリジェンスをオンデマンドで提供し、IT システムと Web アプリケーションの監査、コンプライアンス、保護の全範囲を自動化することで、企業がセキュリティ運用を簡素化し、コンプライアンスのコストを削減するのに役立ちます。

1999 年に設立された Qualys は、アクセンチュア、BT、コグニザント・テクノロジー・ソリューションズ、ドイツテレコム、富士通、HCL、HP Enterprise、IBM、インフォシス、NTT、Optiv、SecureWorks、タタ・コミュニケーションズ、ベライゾン、ウィプロなどの大手マネージド・サービス・プロバイダーやコンサルティング組織と戦略的パートナーシップを結んでいます。また、Cloud Security Alliance(CSA)の創設メンバーでもあります。 詳細については、www.qualys.com をご覧ください。

Qualys サポート

Qualys は、最も徹底したサポートを提供することをお約束します。Qualys は、オンラインドキュメント、電話によるヘルプ、および直接の電子メールサポートを通じて、お客様の質問に可能な限り迅速に回答できるようにします。週 7 日 24 時間体制でサポートを提供しております。

www.qualys.com/support/ でサポート情報にアクセス下さい。

VMDR OT の概要

Qualys VMDR OT は、産業用制御システムのリアルタイムのアセットインベントリ、ネットワークの可視性、脆弱性管理を提供します。Qualys VMDR OT は、直感的なインターフェースと完全に自動化されたリスク評価ワークフローにより、コストのかかる危険なサイバーセキュリティ侵害のリスクを軽減するための強力なツールとして機能します。Qualys は、IT&OT アセットインベントリ、脆弱性管理、ポリシーコンプライアンス、OT エンドポイントベースの脅威検出と対応のすべてに、単一のアプリケーションと単一の画面を提供します。

はじめに

インダストリアル IoT(IIOT)とスマートマニュファクチャリングは、総合設備効率(OEE)とコスト削減を大幅に向上させます。しかし、急速なデジタル化と、以前はエアギャップだった産業環境と企業ネットワーク間の相互接続性が新たに確立されたため、企業がサイバー攻撃にさらされる可能性も高まります。産業用アセットには、より高い可用性と信頼性の要件があります。それらの機能と誤動作は、重大な物理的安全事故につながる可能性があります。これらのシステムへの変更や更新プログラムのインストールによって発生するダウンタイムは、サービスの中断を最小限に抑えるために慎重な計画が必要です。

通常、産業プロセスは、さまざまな産業ベンダーによって製造され、Ethernet/IP、Modbus TCP、Siemens S7 Comm、S7Comm Plus、Profinet、BACnet、DNP3 などのさまざまな産業用プロトコルによって駆動される複数の機器によってサポートされています。これらのプロトコルの多くは、基本的な認証と暗号化が欠如しており、設計上安全ではないため、これらの環境で可視性と定期的なリスク評価を実施することがさらに重要になります。

VMDR OT セキュリティは、サイバー攻撃者からの脅威から産業用制御システムを保護することと定義されています。これは、OT セキュリティと呼ばれることがよくあります。これには、アセットのインベントリと検出、脆弱性管理など、幅広いプラクティスが含まれます。

ネットワークの脆弱性を特定することは、最も重要なステップです。Qualys VMDR OT は、既存の脆弱性を特定し、サイバーリスク軽減ソリューションを推奨します。

Purdue モデルは、VMDR OT の参照アーキテクチャ モデルです。システムを複数のレベルに分割します:Purdue レベル 0 から Purdue レベル 5 まであります。

次の Purdue レベルの参照モデルに示すように、VMDR OT は、すべての Purdue レベルでアセットインベントリ、ネットワークの可視性、および脆弱性の態勢を提供します。

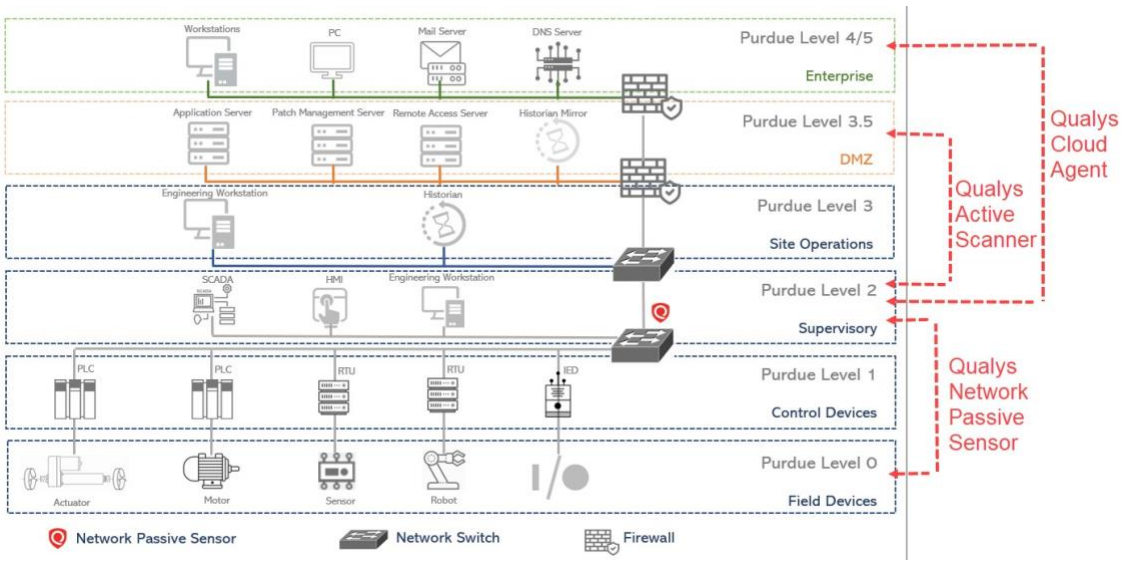
Qualys ネットワーク パッシブ センサー は、ネットワーク スイッチのミラー ポートに設置して、Purdue レベル 0、1、2 に存在するアセットからのトラフィックを確認し、トラフィックを受動的にリッスンし、プロトコルを分析し、アセットインベントリを構築できます。

Qualys Active Scanner は、レベル 2、3、および 3.5 に存在するエンドポイントをスキャンして、すべてのエンジニアリングワークステーションと SCADA サーバー、オペレーティングステーション、製造実行システム、ERP、RTU のジャンプボックスなどのサイト操作機器を処理できます。

Qualys Industrial Control System を使用して、OT デバイス スキャンを起動し、OT アセットとセキュリティ体制に関する最新のビューを取得します。VM/VMDR で OT デバイス スキャン機能を使用できます。OT デバイススキャンは、安全なアクティブスキャンのために提供されています。これは、ID 関連の属性をフェッチするプロトコル指向のスキャンです。VMDR OT は、VM/VMDR からデータを収集し、情報を抽出して脆弱性を検出します。OT デバイス スキャンの詳細については、脆弱性管理のオンライン ヘルプを参照してください。

これらの環境にデプロイされた **Qualys Cloud Agents** は、脆弱性の継続的な可視性と継続的なポスチャを提供できます。

VMDR OT アウトオブバンド構成評価 は、アセットインベントリの構築にも使用できます。これは、他の方法(Qualys ネットワーク パッシブ センサーまたは Qualys Cloud Agent)でアセットインベントリを作成できない場合に便利です。



Qualys アプリケーションで使用可能な VMDR OT 機能を表示するには、次の表を参照してください.

Purdue Level	Assets	Feature	Supported by	Available on Qualys Applications
Purdue Levels 0/1/2	Hardware like PLC, RTU, IO, Robots, VFDs etc	Asset Inventory	Qualys Network Passive Sensor	VMDR OT
		Vulnerability Management	VMDR OT Out of band configuration assessment	

Purdue Levels 2 and above	OT/ICS OS-based endpoints hosting ICS Vendor software - (Engineering workstations, Operator Stations, HMI Servers, DCS Servers, etc.)	Asset Inventory	VMDR application (VMDR OT safe active scan support in Qualys Scanner and Cloud Agent)	VMDR CSAM For more details, see OT Device Scan details
		Vulnerability Management	VMDR (OT/ICS OS-based endpoints hosting ICS Vendor software)	VMDR
		Policy Compliance	Policy Compliance application IEC 62443 NERC CIP Policy	Policy Compliance

Qualys VMDR OT が選ばれる理由

リアルタイム VMDR OT アセットインベントリ

Qualys VMDR OT は、複数のエンジンを介して包括的なリアルタイムのアセットインベントリを構築します。

- Qualys Network Passive Sensor は、産業用プロトコルを分析し、特にフィールドおよび制御ネットワーク層で、さまざまな Purdue レベルを可視化します。

- Qualys は、スキャナー機能を拡張して、産業用プロトコルの安全な VMDR OT 検出を実行します。この新しいスキャンは安全を重視して設計されており、産業用プロトコルと同じ言語で通信し、デバイスが理解できるプロトコル言語でデバイスにクエリを実行します。
- VMDR OT 帯域外構成評価: プログラミングおよびメンテナンス ソフトウェアから収集されたプロジェクト ファイルを使用してアセットをインポートします。

広範な産業用プロトコルのサポート

Qualys VMDR OT は、S7Comm、S7comm Plus、Profinet、Ethernet IP、BACnet、Modbus TCP、DNP3、MQTT、IEC 104、CIP、IEC 61850-MMS、Beckhoff ADS、Omron、PCCC、Niagara Fox など、幅広い IT および OT プロトコルをサポートしています。

帯域外構成評価

Qualys は、アウトオブバンド設定評価をサポートしています。アセット情報は、プログラミングおよびメンテナンスソフトウェアから収集されたプロジェクトファイルを使用してインポートできます。VMDR OT アプリケーションは、アップロードされたファイルを貴重なデータで解析し、収集したデータからアセットを作成します。Qualys は、Omron CX Programmer(.cxp)、Rockwell RSLogix 500(.RSS)、ロックウェルスタジオ 5000(。L5X)、ロックウェルシステムフェレット(.XML)、シーメンス DIGSI 4 (.zip)、シーメンス DIGSI 5 (.zip)、シーメンス DIGSI 5 (.dz5) などをサポートしています。

堅牢な脆弱性管理

Qualys VMDR OT は、検出されたすべての産業アセットに対して継続的な脆弱性評価を提供します。ハードウェアおよびファームウェアベースの脆弱性は、PLC、IO、HMI、ドライブなどに影響を与え、SCADA サーバー、エンジニアリングソフトウェア、HMI ソフトウェアなどに影響を与えるソフトウェアの脆弱性は、パッシブセンサーと Qualys スキャナー、またはクラウドエージェントの組み合わせによってカバーされます。

リスク スコアは、アセットの重要度、脆弱性の重大度、およびアセットの冗長性の可用性に基づいており、優先順位付けと修復アクションの改善に役立ちます。

幅広い産業ベンダーサポート

Qualys VMDR OT は、シーメンス、ロックウェル・オートメーション、シュナイダーエレクトリック、Wago、ジョンソンコントロールズ、ナイアガラ・フォックス、ベッコフ、オムロン、ABB などの主要な業界ベンダーをサポートしています。

概念と用語

VMDR OT アプリケーションで使用される一般的な用語について理解します。

用語	説明
QID	これは、脆弱性に割り当てられた一意の Qualys ID 番号です。
QQL	検索クエリを構築するための Qualys クエリ言語 (QQL) は、Qualys データベースから情報を取得するために使用されます。
Severity Score	Qualys は、ナレッジ ベースのすべての脆弱性に、その悪用に関連するセキュリティ リスクによって決定される重大度スコアを割り当てます。
CVE ID	CVE (Common Vulnerabilities and Exposures) には、一般に知られている脆弱性とエクスポージャーの一般的な名前がリストされています。これらは、この脆弱性チェックに関連する CVE 名です。
Confirmed vulnerabilities	これらは、QualysGuard によって明確に特定された脆弱性です。
Potential vulnerabilities	これらは、完全には検証できない脆弱性です。このような場合、脆弱性の必要条件が少なくとも 1 つ検出されます。
CVSS	共通脆弱性評価システムは、脆弱性の深刻度とリスクを伝えるために設計された業界のオープンスタンダードです。

必須要件

産業用制御システムアプリケーションには、VMDR、サイバーセキュリティアセット管理(CSAM)、および Qualys ネットワークパッシブセンサー(NPS)アプリケーションのサブスクリプションでアクセスできます。

Qualys VMDR OT はどのように機能しますか?

VMDR OT は、Qualys ネットワーク パッシブ センサーを搭載しています。すべてのネットワークトラフィックを継続的に監視し、アセットアクティビティにフラグを立てます。ネットワークに接続された瞬間にデバイスを識別し、プロファイリングします。

Qualys Network Passive Sensor(NPS)は、アクティブにスキャンできない産業環境のアセットを特定します。Qualys Network Passive Sensor(NPS)は、最近開いているポート、トラフィックの概要、ネットワークサービス、使用中のアプリケーションなどの詳細を追加して、既存のアセットインベントリを強化します。アセットインベントリを更新すると、アセットとそのネットワーク上のアクティビティをリアルタイムでより深く理解するのに役立ちます。

アセットの検出とインベントリの収集 – Qualys ネットワーク パッシブ センサー(NPS)がネットワークに展開および設定されると、ネットワーク トラフィックの受動的リッスンを開始し、ト

ラフィックから分析された情報に基づいてアセットを作成します。導入の詳細については、『Qualys ネットワーク パッシブ センサーの導入』を参照してください。

時間の経過とともに、ネットワーク上でさまざまなアセットアクティビティが見られるため、パッシブ センサーは追加のコンテキスト情報を使用してアセットインベントリ属性を強化し続けます。完全なアセットコンテキストの構築にかかる時間は、産業用プロトコルの種類と、環境内で実行されるアクティビティの種類に基づきます。

アセット検出を迅速化するには、「デバイス検出方法を使用したトラフィックの生成」の項を参照してください。

アセットインベントリは、プログラミングおよびメンテナンス ソフトウェアから収集されたプロジェクト ファイルを使用して、VMDR OT 帯域外構成評価を使用して作成することもできます。詳しい情報は、 アセットのインポート を参照してください。

検出と監視 - Qualys ネットワーク パッシブ センサー (NPS) は、デバイスのアクティブなプローブを行わずにネットワーク アクティビティを監視して、ネットワーク内のアクティブなアセットを検出します。VMDR OT アセットインベントリは、Qualys ネットワーク パッシブ センサー (NPS) によってフラグが立てられたアセットアクティビティに応じて継続的に更新されます。VMDR OT アセットインベントリの詳細については、「アセット 」タブを参照してください。

サーバーとクライアント間の通信を表示するネットワークトラフィックを表示するには、「ネットワークトラフィックの表示」セクションを参照してください。

産業アセットの脆弱性が検出され、[脆弱性]タブに一覧表示されます。詳細については、「脆弱性の表示」セクションを参照してください。

VMDR OT の使用を開始する

VMDR OT インベントリの構築を開始するには、次の方法で開始します。

- Qualys ネットワーク パッシブ センサー (NPS) の展開
- VMDR OT アウトオブバンド構成評価を使用したアセットのインポート
- ネットワークデバイスを設定および管理するためのプログラミングソフトウェアからのデバイス検出方法を使用したトラフィックの生成

ユーザーの役割と権限

ユーザーを作成し、定義された役割に従ってアクセス権を付与する役割を割り当てることができます。複数のユーザーロールをサポートしています。

Manager Users	最も権限のあるユーザーは Manager ユーザーです。サブスクリプション内のすべてのリソースに対する完全な権限とアクセス権があります。 ユーザーを作成し、ロールを割り当てることができるのは、Manager ユーザーのみです。マネージャー ユーザーは、ユーザーがアプリケーションにアクセスする方法を選択できます。
Users	ロールに割り当てられた権限に応じて、ユーザーをすべての権限または読み取り専用権限で分類できます。

新規ユーザー: スコープと権限

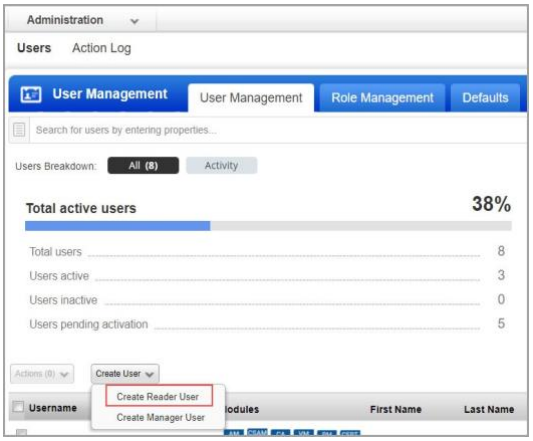
新しいユーザーを作成して権限を付与する権限を持っているのは、Manager ユーザーのみです。

大まかな手順を見てみましょう。

1)ユーザーの作成

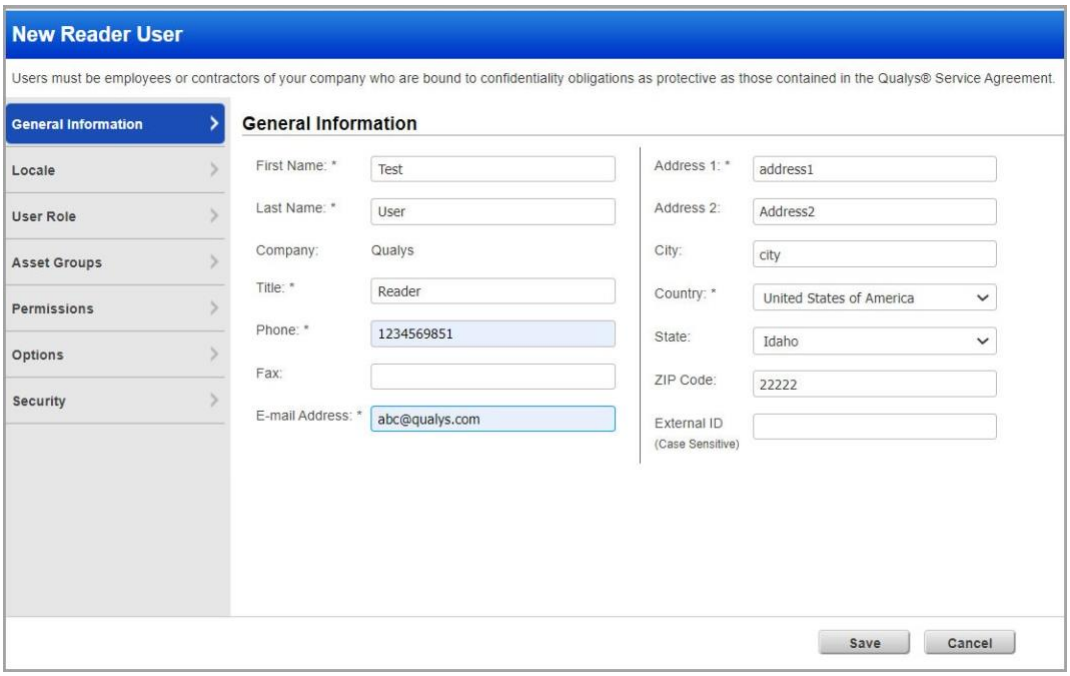
管理アプリケーションを使用して新しいユーザーを作成する必要があります。マネージャは、サブスクリプションサービスレベルで許可されている数までユーザーを追加できます。以下の手順に従います。

1. **Administration module** > **User Management** > **Create User** > **Create Reader User** へ移動します。



一般情報、ロケール、ユーザーロール、アセットグループ(オプション)、権限、オプション、セキュリティなど、ユーザー作成に必要な情報を入力します。

[User Role] で [Reader role] 以上を選択していることを確認します。その他のオプションについては、デフォルト設定をそのまま使用できます。



「保存」をクリックします。

2．ユーザーにアクセス許可を付与する

ロールを定義し、この定義済みロールをユーザーに割り当てることができます。定義するロールによって、ユーザーに割り当てられる権限が決まります。これを行うには、ユーザーのアカウントを編集します。たとえば、フルアクセス権を持つユーザーを作成するには、ロールの

すべての権限を有効にし、そのロールをユーザーに割り当てる必要があります。ロールを割り当てて、一度に複数のユーザーにフルアクセスを割り当てることができます。

3．新しいユーザーを追加した後の検証

新しいユーザーを作成すると、そのユーザーは [アクティブ化の保留中] の状態でユーザー アカウントの一覧に表示されます。ユーザーには、新しいアカウントの資格情報とログイン手順への安全な 1 回限りのリンクが記載された登録メールが届きます。登録メールは、ユーザーのアカウントで定義されたメールアドレスに送信されます。初回ログイン後、ユーザーのステータスが [アクティブ] に変わります。

注:連絡先ユーザーの役割を持つユーザーは、ログイン資格情報を受け取らず、アプリケーションにログインできません。

4．ユーザーへのロールの割り当て

(管理職)管理ユーティリティ(アプリケーション セレクタの最後のオプション)を使用して、ユーザーを表示および管理し、VMDR OT アプリケーションへのアクセス権を付与します。[ユーザー管理] タブでは、各ユーザーがアクセスできるアプリケーションを確認できます。アクセスはロールベースです。

詳細については、管理ユーティリティのオンラインヘルプを参照してください 。

さまざまな役割を知る

次の 2 種類のユーザ ロールを設定できます。

- **すべての権限を持つユーザー**: VMDR OT ユーザーという名前の事前定義されたロールが用意されています。必要なユーザーにロールを割り当てます。
- **閲覧者権限を持つユーザー**: 閲覧者ロールを持つユーザーは、VMDR OT モジュールに表示されるデータのみを表示できます。「新規ロール」をクリックします。ロールに名前と説明を付け、ロールの割り当て時にユーザーに付与する特権に対するモジュールと権限を選択します。

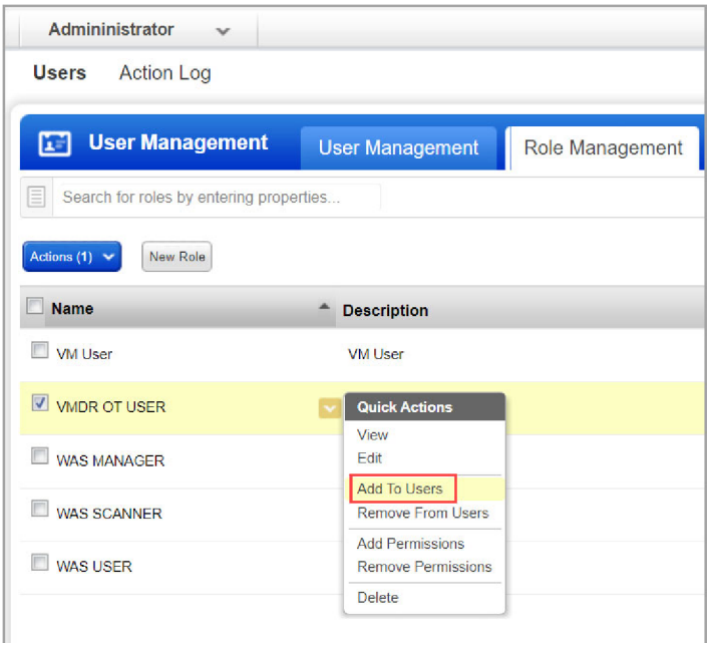
ユーザーへのロールの割り当て

新しいロールを作成したり、既存のロールの権限を変更したりできます。また、ここからユーザーにロールをすばやく割り当てることもできます。

注: 「ロール管理」タブを表示するには、完全な権限とスコープを持っているか、管理ユーティリティで「ロール管理セクションへのアクセス」権限が有効になっているロールが必要です。

1. 管理ユーティリティで、**[ユーザ]** > **[ロール管理]** に移動します。
2. 割り当てるロールを選択し 、「クイックアクション」メニューから「ユーザーに追加」を選択します。
3. ロールを割り当てるユーザーをリストから選択し、「保存」をクリックします。

同様の方法でユーザーからロールを削除できます - アクション「ユーザーから削除」を選択する必要があります。



ロールの編集

1. 一覧から任意のロールを選択し 、**クイックアクション**メニューから編集を選択します。

ロールの名前と説明を変更したり、割り当てられた権限を編集したりできます。ロールに加えた変更は、そのロールが割り当てられているすべてのユーザーに適用されます。

警告 - ロールから UI アクセス許可を削除するときは注意してください。ユーザーは、UI アクセス権限が割り当てられているロールが少なくとも 1 つない場合、UI にログインできません。

権限の編集

ロールの権限を編集する際に、アプリケーションへのアクセス、アクセス可能なモジュール、および現在のロールを持つユーザーのモジュール内の権限を定義できます。現在、2 種類のユーザーを構成できます。ロールに割り当てる権限に応じて、ユーザーをすべての権限または読み取り専用の権限で分類できます。

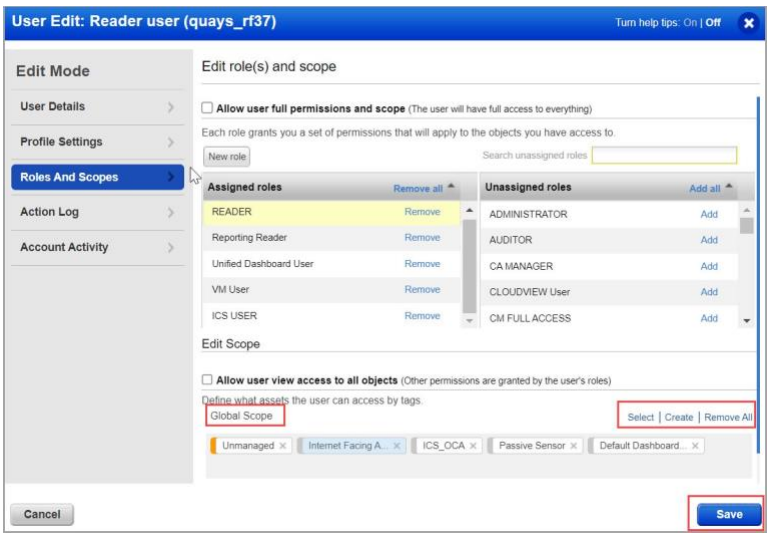
ユーザーがアクセスできるように VMDR OT モジュールが割り当てられていることを確認します。グループのタイトルをクリックすると、その権限が展開されます。次に、ロールに割り当てる権限を選択します。

スコープ内のアセット、脆弱性、およびネットワークリストビューを表示するには、ユーザーがアセットにアクセスできる必要があります。ユーザーがこれらのアセットにアクセスできることを確認します。

ユーザーのスコープにタグを追加する

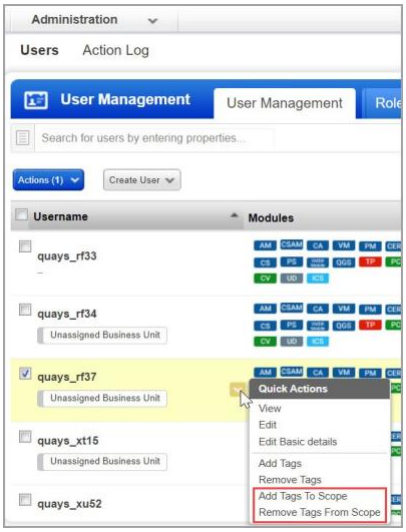
ユーザースコープにタグを追加することで、アセットへのアクセスを提供できます。各アセットには、いくつかのタグを関連付けることができます。独自のタグを作成し、アセットに割り当てることができます。スコープは、Manager ユーザーが他のユーザーに割り当てることができます。マネージャ ユーザは、管理ユーティリティを使用してログインし、タグをユーザ スコープに割り当てることができます。タグの詳細については、「アセットのタグ付け」を参照してください。

1. 管理ユーティリティで、「ユーザー管理」タブに移動し、権限を割り当てるユーザーを選択して「編集」をクリックします。
2. 「編集」ウィンドウで、 左ペインの「ロールとスコープ」タブに移動し、「グローバルスコープ」からタグ(ユーザーがアクセスする必要があるアセット)を選択します。



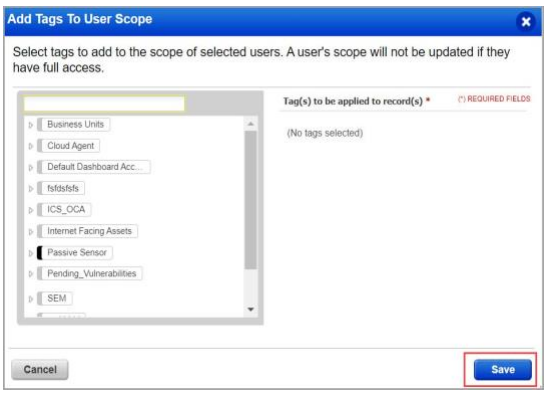
又は

「ユーザー管理」タブのユーザーの「クイック・アクション」メニューから、タグをスコープに割り当てることもできます。



3. リストからタグを選択します。

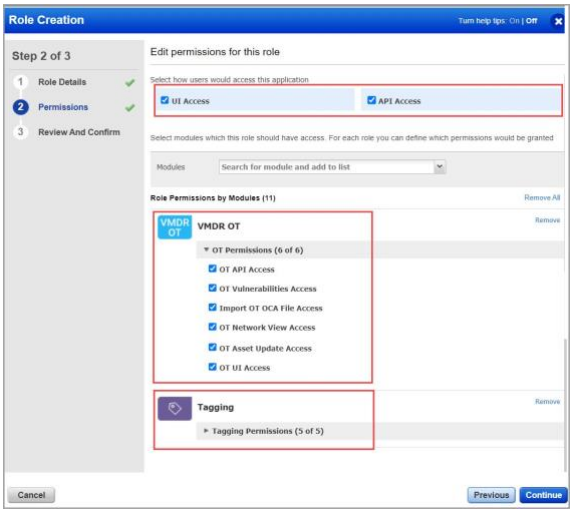
4. 「**保存**」をクリックすると、必要なユーザーにユーザー権限が割り当てられます。



注: アクティビティのタグ付けに関連する権限が必要です。Create User Tag |ユーザータグの編集| ユーザータグの削除 |Dynamic Tag ルールの変更|タグを追加/削除します。

タグ付け権限の詳細については、管理ユーティリティのオンラインヘルプの「タグ付け権限の割り当てまたは削除の手順」を参照してください。

- すべての権限:ユーザーは、他のユーザーの作成と管理を除き、VMDR OT のすべての権限を持ちます。



- 閲覧者権限: 閲覧者ロールを持つユーザーは、VMDR OT モジュールに表示されるデータのみを表示できます。

タグ付け権限の詳細については、管理ユーティリティのオンラインヘルプの「タグ付け権限の割り当てまたは削除手順」を参照してください。

複数のロールの権限の追加/削除

1 回の操作で複数のロールの権限を追加または削除できます。変更するロールを選択し、[クイック アクション] メニューを選択します。

ロールの削除

ロールを選択し 、「クイックアクション」**メニューから「削除**」を選択します。

削除したロールは、ユーザーに割り当てられなくなります。このアカウントは、(以前に割り当てられていた) すべてのユーザーのアカウントから自動的に削除され、それらのユーザーにはロールによって付与されたアクセス許可がなくなります。

注: 事前定義されたロールの権限を編集したり、事前定義されたロールを削除したりすると、編集したロールに関連付けられているユーザーのアクセス動作に違いが生じる可能性があります。

1 回の操作で複数のロールの権限を追加または削除できます。変更するロールを選択し、[クイック アクション] メニューから [アクセス許可の追加] または [アクセス許可の削除] を選択します。

Qualys ネットワーク パッシブ センサーの展開

Qualys ネットワーク パッシブ センサーをネットワークに展開すると、デバイス ID に関連するトラフィックのフローがネットワーク上で生成された後、ネットワーク デバイスのメタデータのスニッフィングが開始されます。収集されたデバイスのプロパティに基づいて、デバイスは Qualys VMDR OT インベントリにアセットとして追加されます。

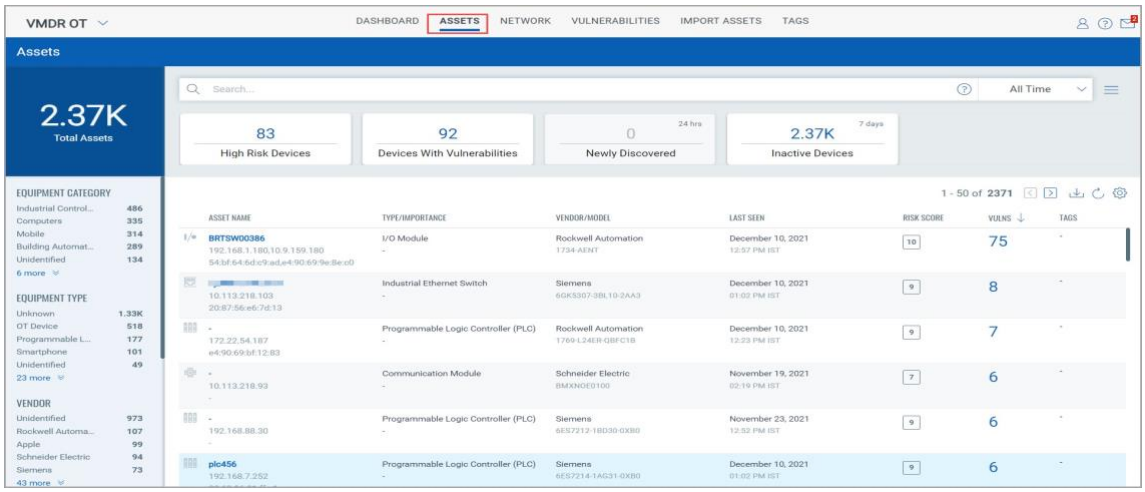
Qualys ネットワーク パッシブ センサーをネットワークに展開し、ミラーリングされたポートをリッスンできるようにします。詳細については、 Qualys Network Passive Sensor Getting Start Guide.

アセットの詳細の表示

「アセット」タブには、産業用アセットの詳細な統合ビューが表示されます。これらは、Qualys ネットワーク パッシブ センサーによって検出およびプロファイリングされる産業用ネットワーク内のデバイスです。

このリアルタイムのアセットインベントリは、アセットメタデータに関連する詳細を提供します。また、脆弱性を事前に管理することで、産業用 OT 環境のセキュリティ体制を評価し、潜在的なサイバーセキュリティの脅威のリスクを軽減するのにも役立ちます。

左上隅には、ネットワーク内の産業アセットの合計数が表示されます。



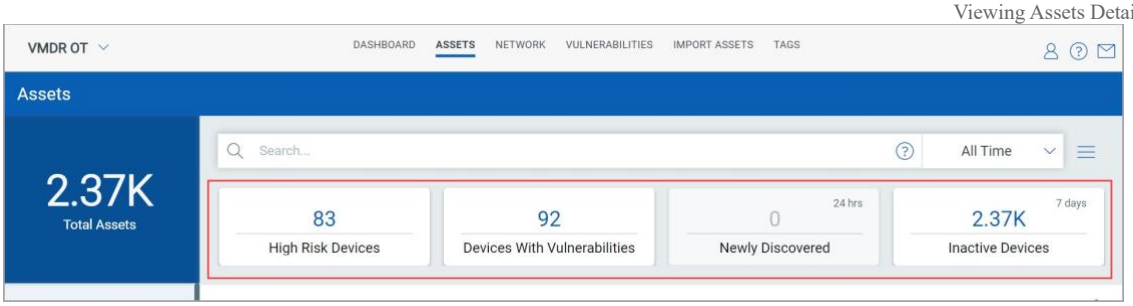
資産テーブルには、検出された資産の一覧と次の詳細が含まれています。

- **アセット名**
- **アセットのハードウェアの種類**
- **ベンダー/モデル番号**
- **アセットアクティビティがネットワーク上で最後に検出された日時**
- **アセットのリスクスコア**
- **アセットで検出された脆弱性**
- **アセットタグ**

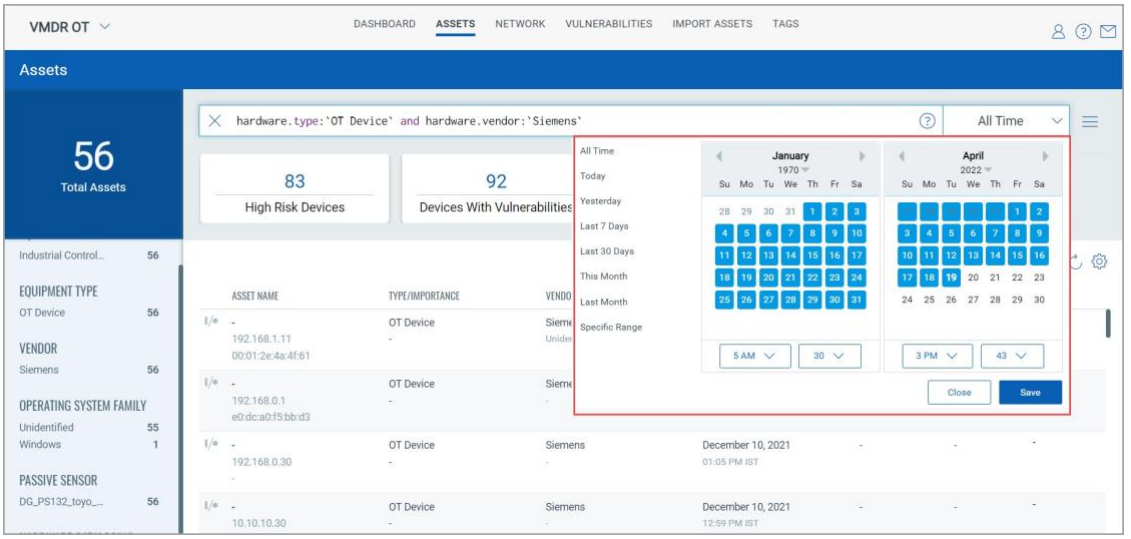
検索バーでは、QQL クエリを作成し、サポートされている検索トークンを使用してアセット検索の範囲を絞り込むことができます。詳細については、 VMDR OT オンライン ヘルプの「VMDR OT のトークンの検索」を参照してください。

左側のウィンドウ フィルターを使用して、備品カテゴリ、備品タイプ、仕入先などのカテゴリにグループ化されたアセットを検索します。選択したカテゴリに属するアセットがアセットテーブルに表示されます。

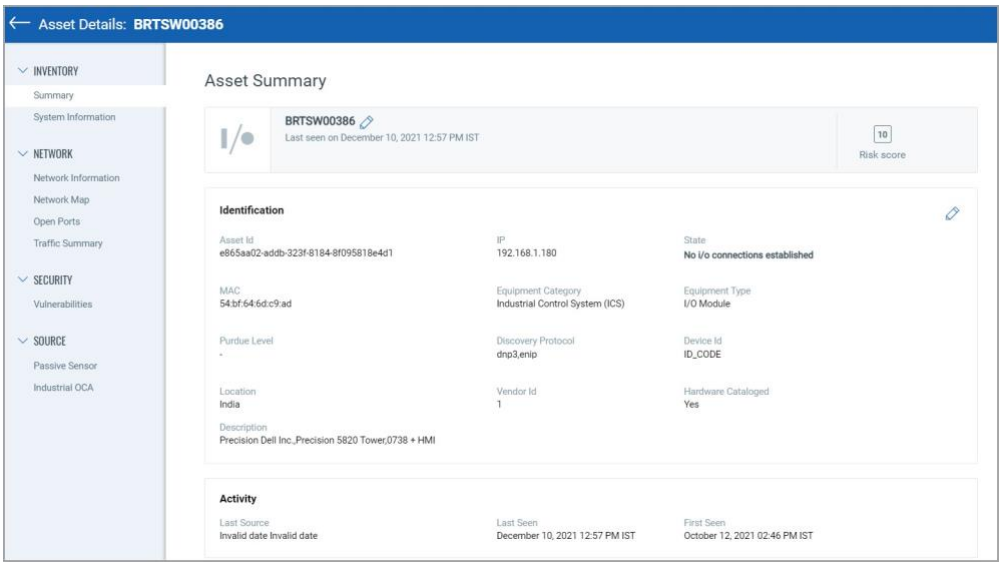
検索バーの下には、リスク スコアの高いデバイス、脆弱性が検出されたデバイス、過去 24 時間以内に Qualys ネットワーク パッシブ センサー (NPS) によって検出されたデバイス、過去 7 日間アクティビティが検出されていないデバイスの 4 つのカテゴリにアセットがグループ化されます。これらの各カードをクリックすると、選択したカテゴリ別にリストされたアセットが表示されます。



検索バーの横にある日付と時間の範囲セレクターを使用して、特定の期間内に検出されたアセットを表示できます。



アセットの詳細を表示するには、アセット名をクリックします。「アセット詳細」ページには、様々なセクションに分かれたアセット情報が含まれています。



次の表に、各セクションの各タブに表示される詳細を示します。

INVENTORY	Summary	Qualys ネットワーク パッシブ センサーがアセットを検出するためのアセット名、ID、IP アドレス、MAC アドレス、機器タイプ、業界プロトコルなどのアセットメタデータ、説明、アセットの割り当てられた場所、最初のパッシブ スキャンの詳細と最後のパッシブ スキャンの詳細など。
	System Information	メーカーの詳細、モデル番号、シリアル番号、ファームウェアバージョン、ハードウェアバージョン、製品コード、アドオンの詳細、プロトコル固有の情報など。
NETWORK	Network Information	IPv4 アドレス、IPv6 アドレス、ドメインの詳細、DNS サーバーの詳細、各インターフェイス上のデバイスと通信するプロトコルなどのインターフェイスの詳細。
	Network Map	選択したアセットのネットワーク マップを表示します。
	Open Ports	開いているポートと、それらのポートで実行されているサービスのリスト。
	Traffic Summary	アセットのトラフィックフローの詳細。これらには、クライアントからサーバ(CTS)およびサーバからクライアント(STC)の日付ごとのトラフィック量の概要、ファミリとボリューム別に分類されたトラフィックが含まれる場合があります。
SECURITY	Vulnerabilities	アセットの潜在的な脆弱性と確認された脆弱性の概要ビュー。
SENSORS	Passive Sensor	アセットを検出した Qualys ネットワーク パッシブ センサーの詳細。
	Industrial OCA	アセットに関する産業用 OCA 情報の詳細。

デバイス検出方式を使用したトラフィックの生成

アセットの検出を高速化するために、デバイス検出方法を使用することもできます。デバイス ID に必要なトラフィックの生成を開始し、デバイス情報を取得します。デバイス情報は、ネットワークデバイスを設定および管理するためのプログラミングソフトウェアから取得されます。

制御システムで追加の設定を行わずにネットワークからトラフィック フローを生成する手順が記載されている『Device Discovery Documents i n VMDR OT Online Help』を参照してください。プログラミングソフトによって手順が異なります。ベンダーのソフトウェアを入手し、デバイスの検出に進みます。

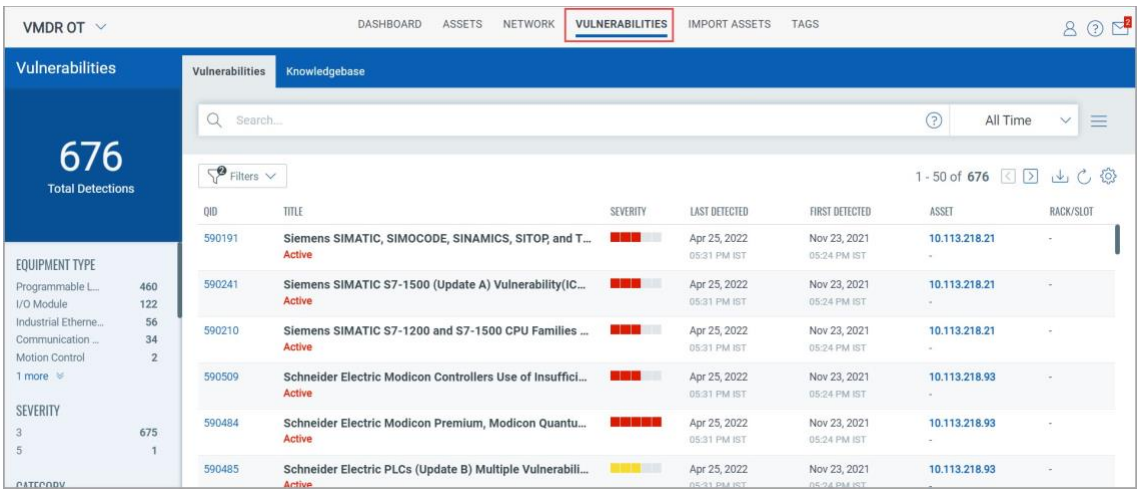
デバイス検出の手順が完了すると、ネットワーク上のデバイス ID に関連する必要なデータフローがトリガーされます。Qualys ネットワーク パッシブ センサーは、このデータをスニッフィングして分析し、Qualys VMDR OT で検出されたデバイスを一覧表示します。

サポートされている OT プロトコルの詳細については、「付録 A - サポートされている OT プロトコル」を参照してください。 サポートされている IT プロトコルの詳細については、「付録 B - サポートされている IT プロトコル」を参照してください。

脆弱性の表示

[脆弱性]タブでは、産業用ネットワーク内のアセットの脆弱性状況の全体像を確認できます。

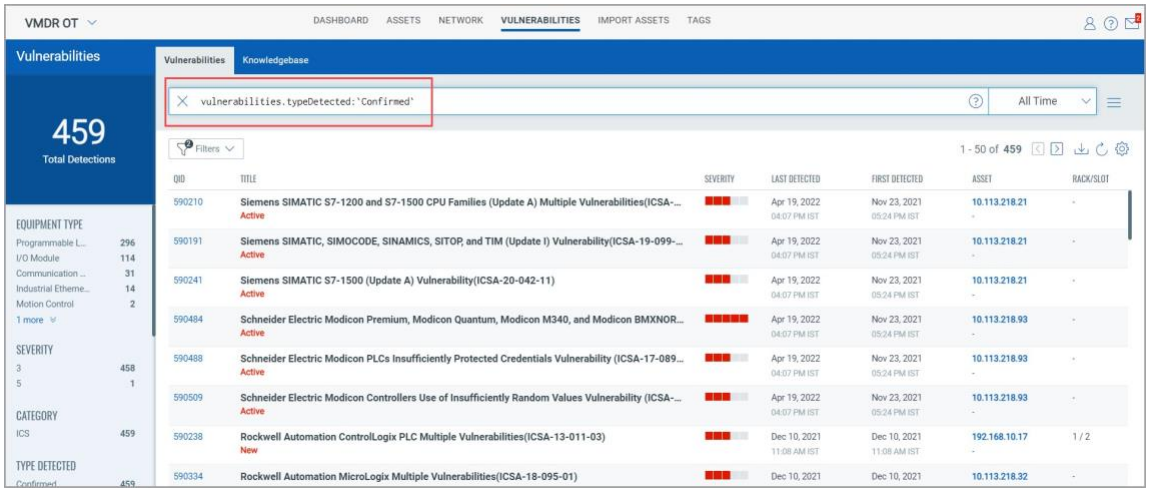
左上隅には、ネットワーク内の脆弱性検出の合計数が表示されます。



脆弱性の表には、検出された脆弱性のリストと次の詳細が含まれています。

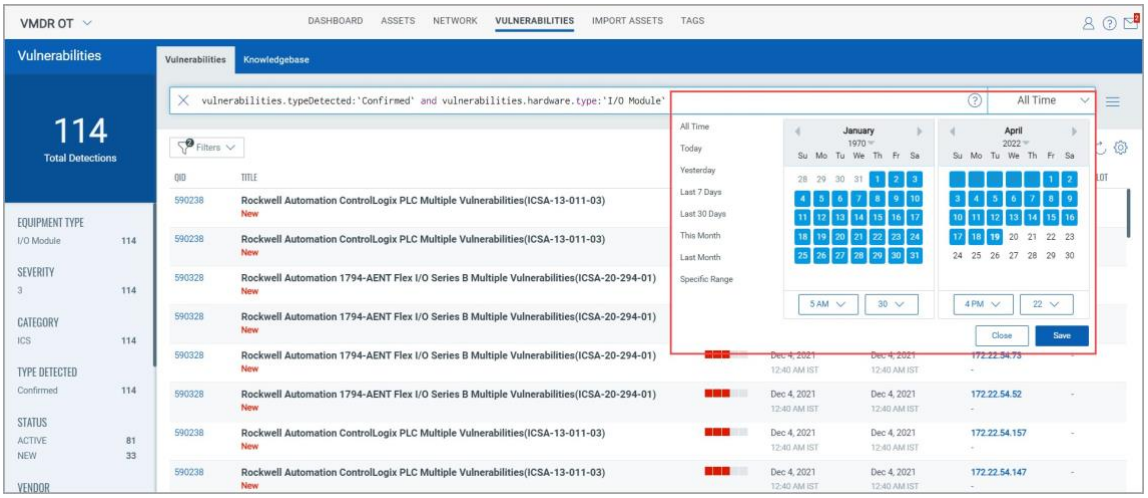
- QID、に割り当てられた一意の Qualys ID
- 脆弱性タイトル
- そのエクスプロイトに関連するセキュリティリスクを詳述します重大度レベル(1～5)
- アセットで脆弱性が最後に検出された日時
- アセットの脆弱性が最初に検出されたとき
- 脆弱性が検出されたアセット
- ラック/スロットの詳細

検索バーでは、サポートされている検索トークンを使用して脆弱性検索の範囲を絞り込むための QQL クエリを作成できます。詳細については、 VMDR OT オンライン ヘルプの「VMDR OT のトークンの検索」を参照してください。左側のペインのフィルターを使用して、様々なカテゴリにグループ化されたアセットを検索します。このリストのカテゴリをクリックすると、選択内容が検索バーの QQL クエリに変換されます。選択したカテゴリに当てはまる脆弱性が脆弱性の表に表示されます。



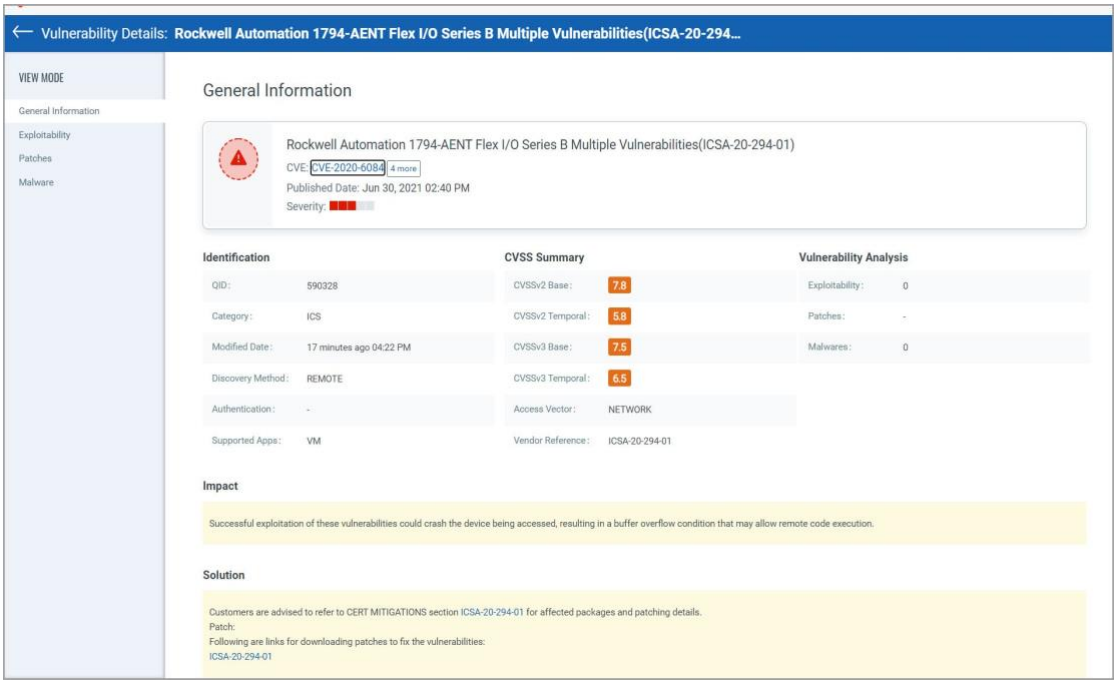
Viewing Vulnerabilities

検索バーの横にある日付と時間の範囲セレクタを使用して、特定の期間内に検出された脆弱性を表示することができます。



脆弱性の詳細を表示するには、**QID** をクリックします。

検出の概要と検出された脆弱性に関する一般情報は、[脆弱性の詳細] ページに表示されます。[脆弱性の詳細] ページには、サードパーティ ベンダーや公開されているソースから入手できる脆弱性に対する既知のエクスプロイト、脆弱性を修正するために利用可能なパッチ、および脆弱性に関連する公開されているマルウェアに関する情報が表示されます。



Viewing KnowledgeBase

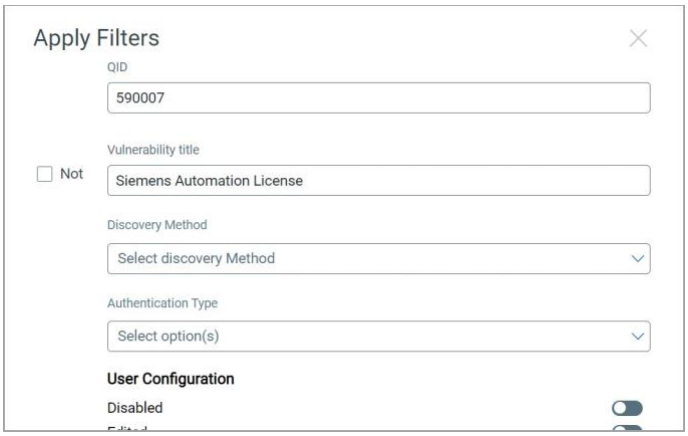
ナレッジベースの表示

セキュリティ業界の脆弱性に関する最新のナレッジベースがあり、継続的に更新されています。

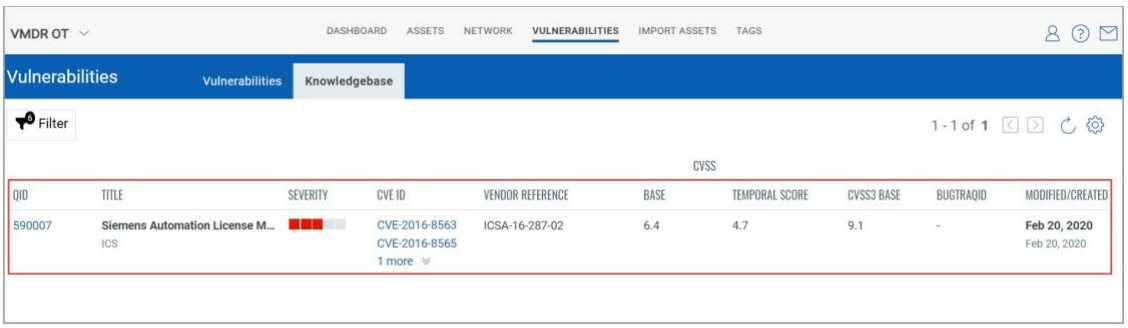
「ナレッジベース」タブを表示するには、「脆弱性」タブに移動し、「ナレッジベース」 をクリックします。

[ナレッジベース] タブには、産業用オートメーション環境で検出できる脆弱性の詳細が含まれています。さまざまな検索フィルターを使用して、脆弱性を見つけることができます。これらのフィルターには、QID、脆弱性のタイトル、検出方法、重大度レベル、カテゴリ、パッチの可用性、CVSS または CVSS v3 スコア、公開日などが含まれます。

[フィルター] をクリックし、[フィルターの適用] で任意のフィルターを選択して [検索] をクリックします。



検索結果は、検索条件に基づいて取得されます。



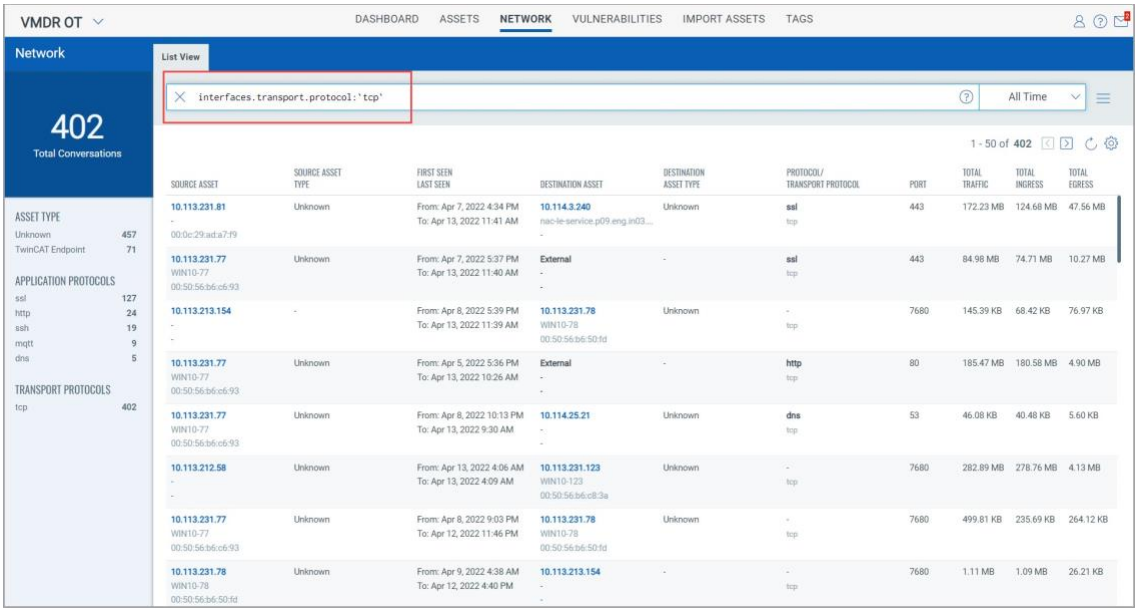
ネットワーク トラフィックの表示

[ネットワーク]タブでは、産業用ネットワーク内のネットワークトラフィックの全体像を確認できます。

複数の Qualys ネットワーク パッシブ センサー(NPS)をネットワーク全体に展開できます。各 Qualys ネットワーク パッシブ センサー(NPS)は、フロー内の送信元と宛先の詳細を含むトラフィックにアクセスできます。[ネットワーク]タブには、特定のポートとプロトコルのすべての送信元と宛先が表示されます。ネットワークリストビューには、ネットワークで使用されているさまざまなプロトコルと、アセットの通信方法が表示されます。

検索バーでは、QQL クエリを構築して、サポートされている検索トークンを使用してネットワークトラフィック検索の範囲を絞り込むことができます。詳細については、 VMDR OT オンライン ヘルプの「VMDR OT のトークンの検索 」を参照してください。

左側のペインのフィルタを使用して、さまざまなカテゴリにグループ化されたネットワーク トラフィックを検索します。 このリストのカテゴリをクリックすると、選択内容が検索バーの QQL クエリに変換されます。 選択したカテゴリに当てはまるネットワーク トラフィックがネットワーク トラフィック テーブルに表示されます。



ネットワークテーブルには、次の詳細を含むネットワークトラフィックのリストが含まれています。

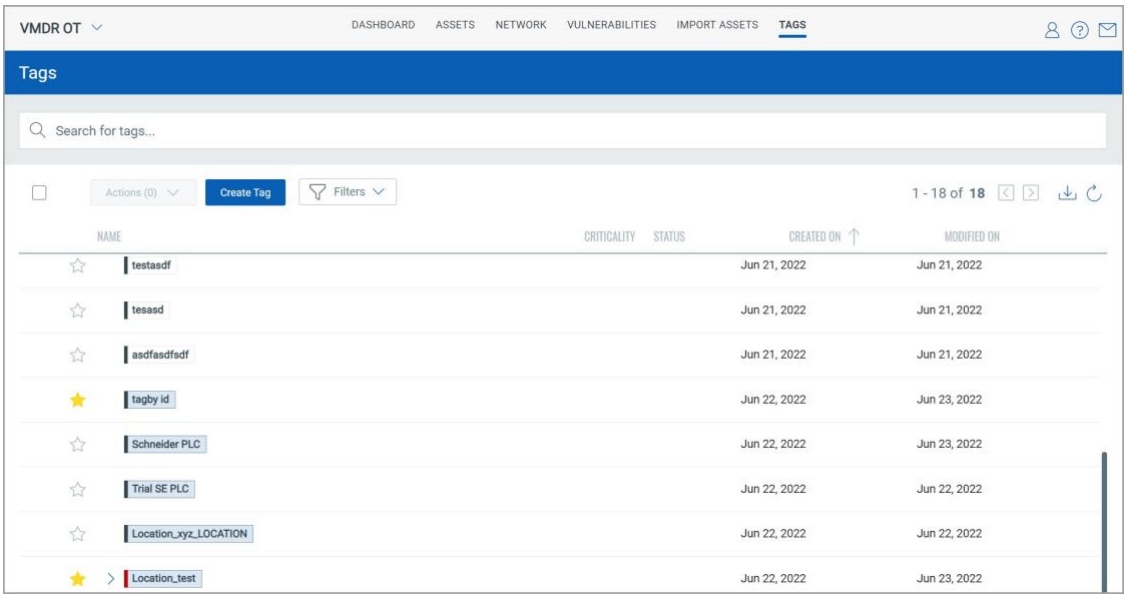
- ソースアセット
- ソースアセットタイプ
- アセットがネットワーク上で観測された最初と最後の日時
- アセットの Destination
- Destination アセットタイプ
- 通信に使用されるプロトコル/トランスポート プロトコル
- 通信しているポート
- ネットワーク上で通信しているネットワークの合計トラフィック量
- ネットワークのイングレス トラフィック量
- ネットワークのエグレス トラフィック

アセットのタグ付け

アセットのタグ付けは、組織内のアセットを整理するのに役立ちます。タグを手動で適用するか、ただし、アセットを論理的、階層的、ビジネスコンテキストのグループに自動的に分類することはありません。タグの最も強力な使用法は、動的タグを作成することで実現されます。ダイナミックタグは、ダイナミックタグ付けルールの検索条件に基づいてアセットにタグを自動的に割り当てます。

「タグ」タブでは、アセットに適用されている様々なタグのリストと、新しいタグを作成するオプションを表示できます。

タグの検索からタグを検索できます。



タグの構成

タグを設定してアセットに適用します。タグは、アセットを整理し、アセットへのユーザーアクセスを管理するのに役立ちます。

1) 「タグ」タブに移動し、「タグの作成」をクリックします。

2) タグの基本的な詳細とタグのプロパティを入力します。

- **基本情報**
    - タグに名前を付けます(最大 1024 文字)。
    - タグをお気に入りとして作成する場合は、[お気に入りとしてマーク] を選択します。お気に入りはリストに黄色の星で表示されます。
    - タグの説明を追加します(省略可)。

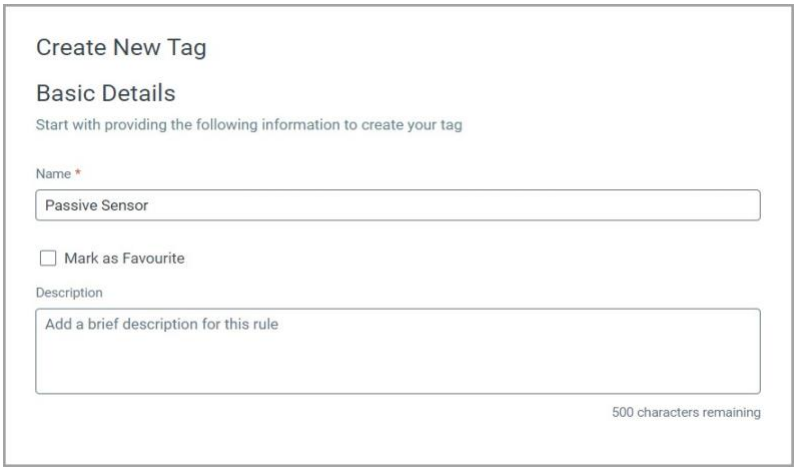
- **タグのプロパティ**

色分けは、タグを整理するのに最適な方法です。タグごとに異なる色を割り当てることができます。子タグを作成する際、アカウント内の既存のタグから親タグを選択できます。

- 既存のタグを選択するには、「選択」をクリックし、「タグの選択」ポップアップからタグを選択します。

また、親の新しいタグを作成することもできます。

- 「作成」をクリックすると 、タグを作成するための類似のフォームが再び表示されます。この新しいタグから新しい親を作成することはできません。



3)ダイナミックタグタイプを設定します(オプション)。動的ルールがない場合、タグは静的タグとして保存されます。

- **タグの種類**

タグには、静的と動的の 2 種類があります。

デフォルトでは、静的タグが作成されます。ダイナミックタグでは、タグルールを定義できます。

「作成時にルールを評価」チェック・ボックスを選択すると、動的ルールが作成または更新された後にそのルールを評価できます。

- **タグルール**

これらは、タグを適用するアセットを識別するのに役立つルールです。

- 動的ルールなし - タグは静的タグになります。
- Asset Name Contains(アセット名に含まれるもの) - ユーザー定義可能なアセット名の一部に、入力した部分文字列が含まれている場合にタグを適用します。「|」で区切られた複数の部分文字列を追加します。(縦棒)で、前後にスペースを入れません。

- アセットインベントリ - VMDR OT のアセットにタグを適用します。
- 範囲内の IP アドレス - 入力した範囲内の IP を持つアセットにタグを適用します (例: 172.31.254.0-172.31.254.25 または 172.31.254.0/25)。
- [範囲内の IP アドレス + ネットワーク] - 入力した範囲とネットワーク内の IP を持つアセットにタグを適用します。
- Open Ports (オープンポート) - ポートリストが入力したポート(例:80,123)と一致するアセットにタグを適用します。
- アセット検索 - 「アセット検索」フィールドで定義された検索条件に基づいて、アセットにタグを適用します。XML コードを使用してクエリを定義できます。

- **選択したアセットに対するルールのテストルールの適用（オプション）** テストするアカウント内のアセットを選択します。

  緑色の「パス」は、アセットがルールに一致することを示します。

  赤色の「失敗」は、アセットがルールに一致しないことを示します。

4) 「**作成**」をクリックしてタグを保存します。

ダイナミックタグを保存すると、定義したルールに一致する検出されたすべてのアバに適用されます。アセットリストをフィルタリングして、新しいタグルールに一致するアセットのみを表示できます。

注: 静的タグを保存すると、[アセット] タブからアセットに適用できます。

動的タグの例を表示するには、オンラインヘルプを参照してください。

アセットタグの管理

タグのクイックアクションメニューから多くのアクションを実行できます 。

機能	手順
View the Tag details	「タグ」タブに移動し、タグの「クイック・アクション」メニューの下にある「表示」をクリックします。
Edit the Tag details	「タグ」タブに移動し、タグの「クイック・アクション」メニューの下にある「編集」をクリックします。
Find Assets with the specific tag	「タグ」タブに移動し、特定のタグの「クイックアクション」メニューの下にある「アセットの検索」をクリックします。「アセットを検索」オプションを選択すると、「アセット」タブに移動し、特定のタグを持つアセットのリストが表示されます。

Move tags to root	「タグ」タブに移動し、子タグの「クイック・アクション」メニューの下にある「ルートに移動」をクリックします。「ルートに移動」アクションを実行すると、子タグは親タグに移動され、ルートに移動する間、その下にあるすべての子が引き継がれます
Mark tag as favorites	頻繁に割り当てるタグがある場合は、それらをお気に入りに追加すると時間を節約できます。新しいタグを追加するとき、または既存のタグを編集するときに、タグをお気に入りとしてマークできます。タグがすでにお気に入りになっている場合は、お気に入りから削除するオプションが表示されます
Remove tag from favorites	「タグ」タブに移動し、特定のタグの「クイックアクション」メニューの下にある「アセットの検索」をクリックします。
Add Child Tag	「タグ」タブに移動し、タグの「クイック・アクション」メニューから「子タグの追加」をクリックします。親タグには、最大 8 つのタグレベルと 100 個の子タグを作成できます。
Delete a Tag	「タグ」タブに移動し、タグの「クイック・アクション」メニューから「削除」をクリックします。削除できるのは、カスタムで作成されたタグのみです
Save the Tags	ダイナミックタグを保存すると、定義したルールに一致する検出済みのすべてのアセットに適用されます。アセットリストをフィルタリングして、新しいタグルールに一致するアセットのみを表示できます。
Save the Static Tag	静的タグを保存すると、[Assets] タブからアセットに適用できます
Use of tag filters	[タグ]タブに移動すると、[フィルター]が表示されます。タグのリストは、お気に入りとスコープ内のチェックボックスを使用してフィルタリングできます。また、タグに適用された色に基づいてタグをフィルタリングすることもできます。

アセットのインポート

アセットインベントリは、VMDR OT 帯域外構成評価を使用して作成することもできます。アセットは、プロジェクトファイルを使用してインポートできます。プロジェクト ファイルは、プログラミングおよびメンテナンス ソフトウェアから収集され、VMDR OT アプリケーションにアップロードされ、アカウントからアクセスできます。VMDR OT アプリケーションは、アップロードされたファイルを貴重なデータで解析し、収集したデータからアセットを作成します。

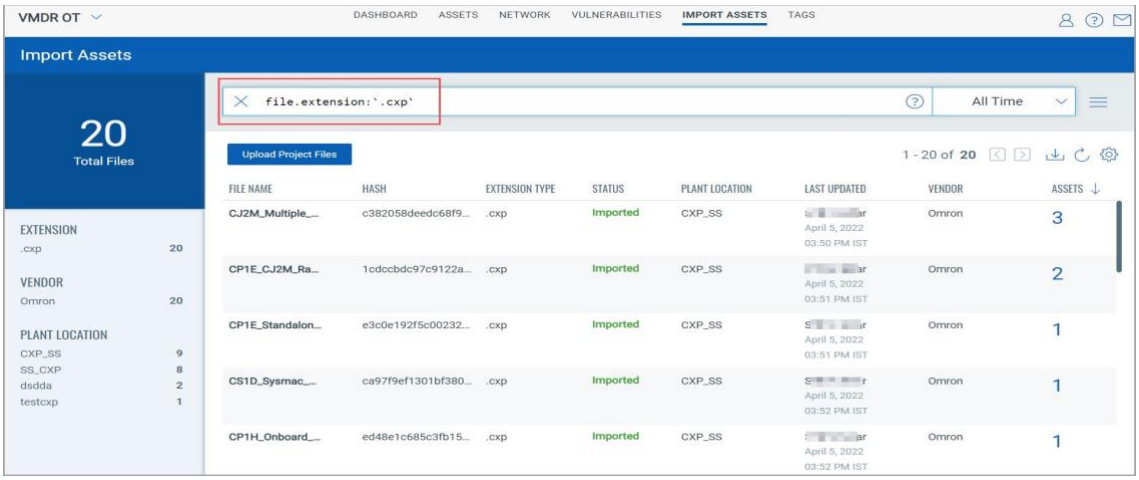
[アセットのインポート]タブには、プロジェクトファイルをアップロードするオプションがあります。プロジェクトファイルは、cxp、zip、Xml、RSS などの拡張子をサポートしています。

プロジェクト ファイルを生成する手順を表示できます。使用するプログラミングソフトによって手順が異なります。Omron CX Programmer (.cxp)、Rockwell RSLogix 500 (.RSS)、ロックウェルスタジオ 5000(。L5X)、ロックウェルシステムフェレット(.XML)、シーメンス DIGSI 4 (.zip)、シーメンス DIGSI 5 (.zip)、シーメンス DIGSI 5 (.dz5) など。

サポートされる OCA の詳細については、「付録 C - サポートされる OCA」を参照してください。

左上隅には、アップロードされたプロジェクトファイルの合計数が表示されます。検索バーでは、サポートされている検索トークンを使用してファイル検索の範囲を絞り込むための QQL クエリを作成できます。詳細については、 VMDR OT オンライン ヘルプの「VMDR OT のトークンの検索」を参照してください。

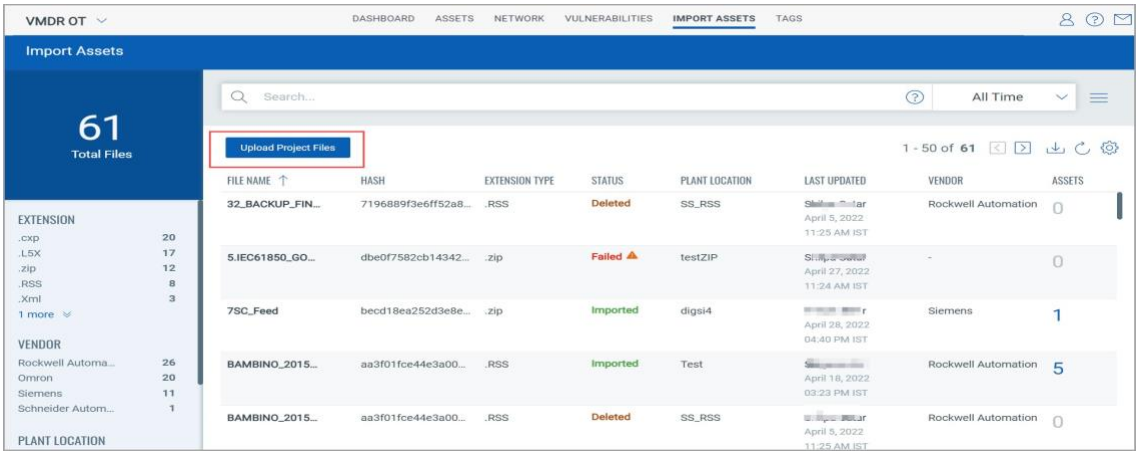
左側のウィンドウ フィルターを使用して、さまざまなカテゴリにグループ化されたファイルを検索します。このリストのカテゴリをクリックすると、選択内容が検索バーの QQL クエリに変換されます。選択したカテゴリに当てはまるファイルがテーブルに表示されます。



インポートアセットテーブルには、次の詳細が含まれています。

- ファイル名
- ファイルのハッシュ
- 拡張子の種類
- 「インポート済み」「インポート中」、「失敗」、「削除済み」などのステータス
- ファイルの収集元のプラントの場所
- ファイルが最後に更新された日時
- ファイルのベンダー
- ファイル内のアセットの総数

ファイルをアップロードするには、「**プロジェクト・ファイルのアップロード**」をクリックします。

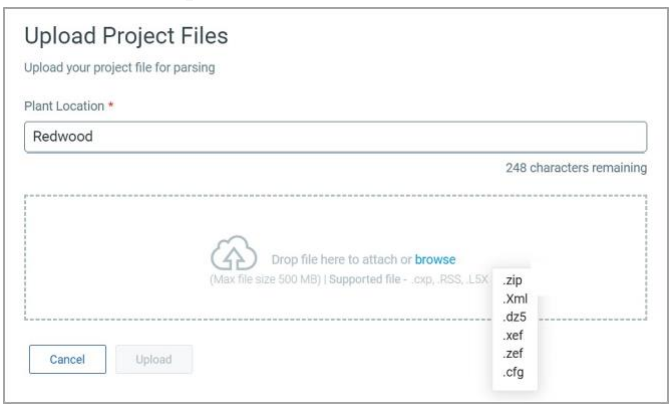


[プラントの場所]名を指定し、[参照]を使用して保存した場所からファイルを選択します。

プロジェクトファイルは、cxp、RSS、zip、Xml、d5Z、zef、xef、cfg などの拡張子をサポートしています。

注:ファイル拡張子は大文字と小文字が区別されるため、アップロードする拡張子がサポートされていることを確認してください。

「**アップロード**」をクリックします。



ファイルがアップロードされ、ステータスが [インポート済み] と表示されます。ファイルのアップロードに応じて、

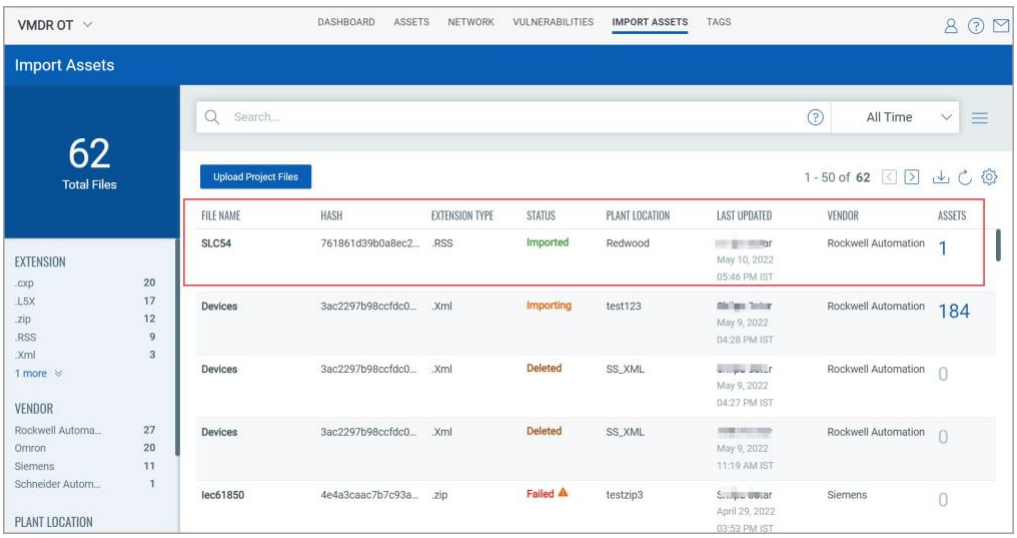
インポート中 - ファイルはまだアップロード中です

インポート済み - ファイルは正常にインポートされました

削除済み - ファイルが削除されました

失敗 - ファイルをインポートできませんでした

プログラミングおよびメンテナンス ソフトウェアからプロジェクト ファイルを生成する方法の詳細については、VMDR OT オンライン ヘルプの「プロジェクト ファイルの生成」を参照してください。

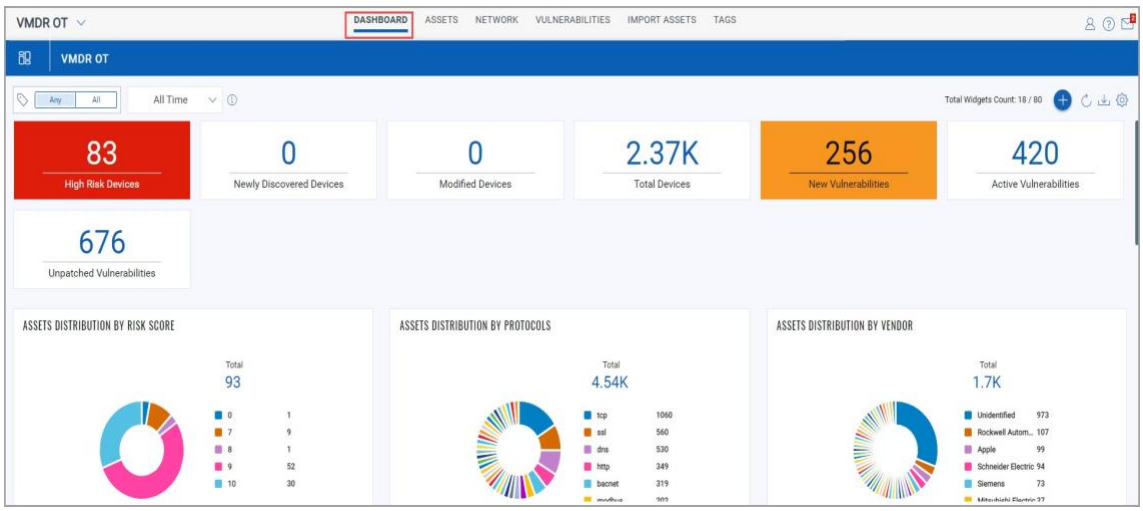


VMDR OT ダッシュボードの管理

アセットと脆弱性の態勢を視覚化するには、ダッシュボードにウィジェットを追加するだけです。[ダッシュボード] タブは、VMDR OT のホーム ページです。

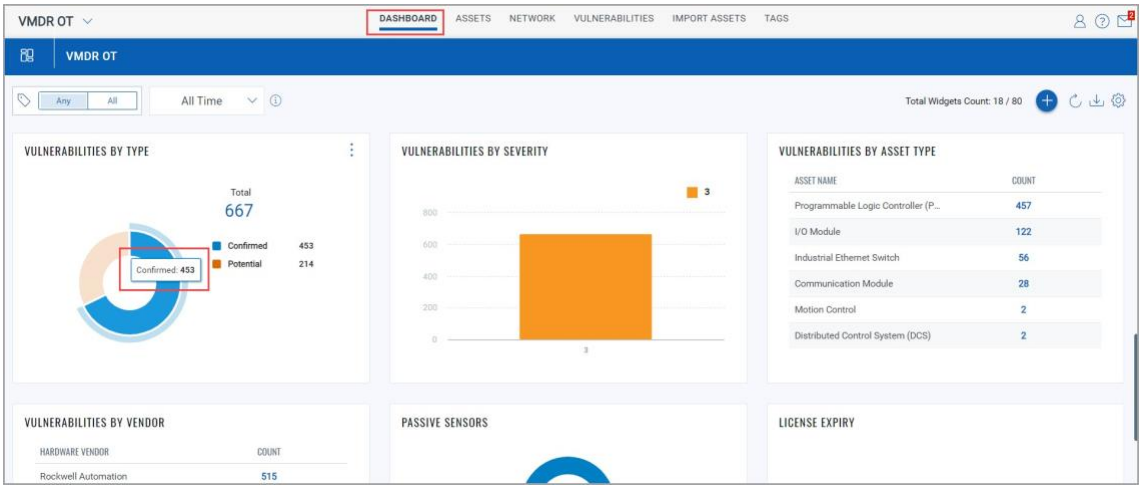
VMDR OT ダッシュボードを表示するには、アプリケーション セレクタから **[VMDR OT]** を選択します。ダッシュボードには、デフォルトで、高リスクデバイス、新しく検出されたデバイス、新しい脆弱性、アクティブな脆弱性などのカウントカードがあります。

リスクスコア別のアセット分布、プロトコル別のアセット分布、ベンダー別のアセット分布、タイプ別の脆弱性、重大度別の脆弱性に基づくさまざまなウィジェットなど、さまざまなウィジェットがあります。ウィジェットの追加を使用して、VMDR OT 関連のウィジェットを追加できます。

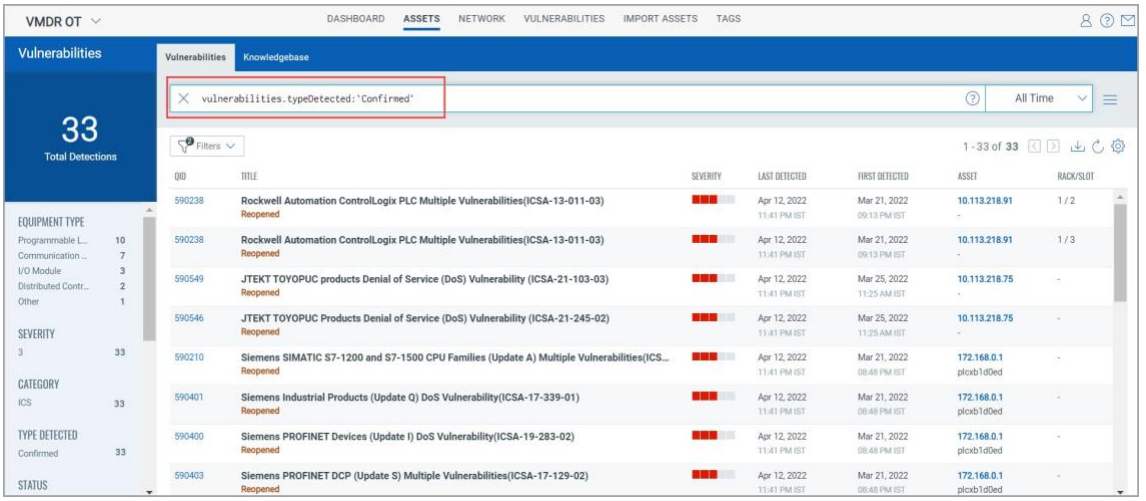


ウィジェットはインタラクティブです。ウィジェットの特定の部分をクリックすると、[関連] タブにリダイレクトされます。

たとえば、上記の VULNERABILITIES BY TYPE ウィジェットで [確認済み] をクリックすると、確認された脆弱性の詳細の [脆弱性] タブに移動します。



確認された脆弱性の詳細がすべて表示されます。



動的ダッシュボードは、情報の表示方法をカスタマイズするのに役立ちます。Qualys には、開始するためのデフォルトのダッシュボードが用意されています。

統合ダッシュボードの表示

ダッシュボードは、アセットを視覚化し、脅威にさらされていることを確認し、保存された検索を活用し、脆弱性の優先度を迅速に修正するのに役立ちます

Qualys VMDR OT は Unified Dashboard (UD) と統合され、すべての Qualys アプリケーションからの情報を 1 か所に集めて視覚化します。UD は、強力な新しいダッシュボードフレームワークとプラットフォームサービスを提供し、他のすべての製品で使用して既存のダッシュボード機能を強化します。

Qualys VMDR OT)には、すぐに使用できるダッシュボードがいくつか用意されています。各ダッシュボードには、提供する情報の簡単な説明が表示されます。他のモジュール/アプリケーシ

ョンから情報を取得してダッシュボードに追加するようにウィジェットを構成するのは簡単です。要件に応じて、多くのダッシュボードを追加してビューをカスタマイズできます。

詳細については、統合ダッシュボードのヘルプを参照してください。

Appendix A - サポートされている OT プロトコル

この付録では、産業用制御システムがサポートする OT プロトコルをリストアップします。

- Siemens S7 Comm	- Omron Fins
- Siemens S7 comm plus	- Mitsubishi Melsoft
- Profinet	- Mitsubishi CC Link
- Ethernet IP	- Mitsubishi SLMP
- CIP (Common Industrial Protocol)	- EtherCAT
- PCCC	- Emerson Delta-V
- Modbus TCP	- Redlion Crimson
- BACnet	- Toyopuc
- Niagara Fox	- Microsoft Discovery Protocol
- Johnson Controls Metasys	- Schneider UMAS
- DNP3	- Honeywell CeeNTComm (C200, C300)
- IEC 104	- Proconos
- IEC 61850 – MMS	- GE-SRTP
- Beckhoff AMS / ADS	- MQTT

Appendix B - サポートされている IT プロトコル

この付録では、産業用制御システムがサポートする IT プロトコルの一覧を示します.

- TCP	- LLDP
- UDP	- UPnP
- DHCP	- SMTP
- HTTP	- SNMP
- DNS	- Netbios
- SSH	- SIP
- SSL	- ARP
- Kerberos	- IPv6 Neighbor Discovery
- CDP	

Appendix C - サポートされている OCA

この付録では、産業用制御システムでサポートされている OCA(帯域外構成評価)をリストします。

Vendor	Engineering Tool	File Extension Type
Beckhoff zip	TwinCAT3	.zip, .tnzip
Emerson	DeltaV Explorer	.fhx
GE Fanuc	Proficy Machine Edition	.zip, .SwxCF
Omron	CX-Programmer	.cxp
Rockwell	RSLogix 500	.RSS
Rockwell	RSLogix 5000/ Studio 5000	.l5x
Rockwell	RS System Ferret	.Xml
Siemens	Digsi4	.zip
Siemens	Digsi5	.zip,.dz5
Siemens	Simatic Manager (Step 7)	.cfg
Siemens	TIA Portal	.zip, .zap(.zap15, .zap15_1, .zap17)
Siemens	LOGO! Soft Comfort	.lnp, .mnp
Siemens	PRONETA	.xml
Schneider	Unity L/XL	.zef, .xef
Schneider	TwidoSuite	.zip, .xtwd
Schneider	Schneider Concept	..ccf, .CCF
Mitsubishi	GX Works3	.gx3
Mitsubishi	GX Works2	.gxw
Red Lion Controls	Crimson	.cd3, .cd31