Industrial Security

極めて精密な ICS、SCADA、製造、その他の運用・制御システムにおける継続的な資産と脆弱性の可視化を実現します。

問題の概要

Tenable の Industrial Security をご利用いただくと高い安全性が求められる運用・制御ネットワークにおける継続的な資産の検出と脆弱性の検知が可能になります。運用・制御技術（Operational Technology: OT）システム向けに設計されたこのソリューションは、パッシブな監視を使用することで安全かつ信頼できる知見を提供します。これにより、自社が何を所有していて、何を保護するべきかについて知ることができます。ICS、SCADA、製造、その他のシステムに幅広く対応する Industrial Security は、IT や OT のセキュリティ、プラントの運用、コンプライアンスを担当する各チームのセキュリティを拡張し、資産の保護を強化し、法規制へのコンプライアンスを徹底するのに役立ちます。また、OT 固有のソリューションとして、システム、アプリケーション、脆弱性の最新の状態を提示し、自社の OT サイバーエクスポージャーについて理解し、運用・制御パフォーマンスを保護するのに役立ちます。

Siemens との戦略的な提携関係に裏打ちされた Tenable の Industrial Security では、電力、ガス、水道などの業種の重要なインフラストラクチャをパッシブに監視することにより、数十社の OT ベンダーのプロトコルやデバイスをサポートするなど、専門的な OT サポートを提供します。セキュリティチームや運用チームが自社の極めて精密なシステムで検出、視覚化、監視を安全な方法で行うことができるのは、この非侵入型のアプローチだけです。

特長

このソリューションの基本的な特長として、次の事項が挙げられます。

- 自社の実稼働ネットワークで機能しているシステム、アプリケーション、サービスおよびそれらのコンポーネント間の接続を全体的に監視します

Tenable の Industrial Security は、非侵入型の方法で資産を継続的に検出し、脆弱性を検知します。また、パケットレベルでネットワークトラフィックを分析することにより、ICS、SCADA、その他の運用・制御システムを奥深くまで可視化します。

このソリューションでは、特許を取得したパッシブ監視テクノロジーを使用して、重要な OT システムの脆弱性を確実に検出します。これにより初めて、自社の実稼働ネットワークにあるエクスポージャーの継続的な可視化が可能となります。

- 精密な ICS、SCADA、製造、その他の運用・制御技術など、途絶のリスクがあってスキャンできないシステムの脆弱性を確実に識別します
- 自社のネットワークに追加された新しい資産を自動的に検出して、そのプロファイルを把握します
- ポイントインタイムの脆弱性スキャンから、継続的な資産と脆弱性の監視へ移行します
- 新しい脆弱性、あるいは新しいシステムや不良システムによって生じた、実稼働中の資産に対する潜在的なリスクを即座に識別します
- サイバーセキュリティと運用・制御技術の世界的なリーダーである Tenable と Siemens がサポートする、OT ネットワーク専用のソリューションを利用します
- OT と IT のセキュリティ対応を同じベンダーに統一することにより、最新のアタックサーフェスを完全に把握することができます

主な機能

資産の継続的な検出

このソリューションでは資産を完全に可視化するために、次のようなネットワークトラフィックを継続的に監視します。

- ICS、SCADA、製造などの幅広い種類のデバイスにわたって、数百にのぼる特定の OT 資産、および、それに関連する通信プロトコルを識別します
  - 承認されていないソフトウェアや管理されていないデバイスを含め、運用・制御環境全体のデバイス、アプリケーション、プロトコルを一括して可視化
  - Siemens、ABB、Emerson、GE、Honeywell、Rockwell/Allen-Bradley、Schneider Electric をはじめとする数十社もの製造業者のシステムをサポート
  - BACnet、CIP、DNP3、Ethernet/IP、ICCP、IEC 60870-5-104、IEC 60850、IEEE C37.118、Modbus/TCP、OPC、openSCADA、PROFINET、Siemens S7 などのプロトコルをサポート
- ネットワークに追加された新しい資産を検出します
- それぞれのアクティブなホストのオペレーティングシステムをパッシブに判別します
- ネットワーク上のマシン間の接続と「通信量の多い」マシンを表示します
- .nessus、.csv、HTML、syslog 形式でのデータエクスポートをサポートします

パッシブな脆弱性の検知

Tenable の Industrial Security は、実稼働ネットワーク全体のサイバーエクスポージャーについての詳細な分析情報を提供します。

- ネットワークトラフィックのパッシブな監視（ディープパケットインスペクション）を通して、幅広い種類の OT 脆弱性を確実に検知します
- 前述のすべての OT 製造業者およびプロトコルについて脆弱性を検知します
- 重大度、数、名前などで分類して資産と脆弱性を示します
- 資産の役割（PLC、PC、サーバー、その他）など、OT 環境の必要に合わせて調整した情報を配信します

複数サイトの管理

このソリューションは、分散型の運用･制御環境をサポートします。

- Industrial Securityの複数のインスタンスから収集したデータをまとめて管理する機能により、複数のサイト/プラントにわたる一元的な可視化を実現します

配信オプション

Industrial Security は、従来型のオンプレミスソフトウェアとして導入することも、Siemens が配信するサービスとして利用することもできます。

詳細情報 **:**tenable.com のサイトをご覧ください
お問い合わせ **:**sales@tenable.com宛てにメールを送信するか、tenable.com/contact のサイトをご覧ください。