＜Nozomi Networks ホワイトペーパ＞

株式会社テリロジー

市場ニーズが OT モニタリング要件を喚起する！

はじめに

OT ネットワークの継続的モニタリングは、あらゆる産業/OT サイバーセキュリティ戦略にとって不可欠な要素である。産業分野の多くの企業は、OT ネットワークに接続されている資産インベントリの見える化とシステムの異常な挙動の迅速なアラート通知の必要性を認識している。こうした将来のニーズの掘起こしに対してどのようにサポートするか。そのためのソリューションを考慮する必要がある。以下のような OT サイバーセキュリティの市場ニーズが台頭している:

- OT セキュリティおよび IT/OT サイバーセキュリティのコンバージェンスに関する企業の CISO がより深い関与を示し始めている。
- 企業 SOC および MSSP などの外部セキュリティサービスプロバイダが立上げ。
- デジタルトランスフォーメーション(DX)化の普及と IIoT 導入の加速。

これらの市場の変化において、OT ネットワークの継続的モニタリングソリューションを企業ユーザが検討する場合のインパクトについて考察する。

CISO の関与と IT/OT コンバージェンス、SOC と MSSP の拡大、デジタル化の動きという 3 つの市場の牽引パワーが、世界の OT セキュリティニーズを根本的に改革する。

1. CISO の関与と IT/OT サイバーセキュリティコンバージェンスに向けて、更なる OT セキュリティの見える化が必要

高額な被害をもたらすランサムウェア攻撃と国家規模のサイバー脅威により、産業系企業の経営者達の間ではサイバーセキュリティの懸念が高まっている。これにより、OT サイバーセキュリティへの CISO の関与が進み始めており、OT サイバーリスクとコンプライアンスサポートに対する見える化の向上が求められている。また、この現象は、すべてのビジネスプロセスにわたるエンドツーエンドのセキュリティガバナンスを取り組むために、IT と OT のサイバーセキュリティプログラムを統合する取り組みを促進する。

ICS ネットワークソリューションは、パッシブモニタリングを通じて資産インベントリ情報を収集するが、これは新たな見える化要件を満たすには十分ではない

CISO は、IT ネットワークスキャンツールが提供する同レベルの詳細とカバレッジをこの ICS ネットワークにも求めている。

これらの要求を満たすために、ICS ネットワークソリューションでは、通信していないデバイスを検出したり、アクティブポート、ソフトウェアバージョンなどの詳細な資産情報を収集するアクティブスキャンが必要である。理想的には、このソリューションは、OT の脆弱性やポリシー違反を含む詳細な OT サイバーリスク評価に関心ある CISO および IT セキュリティチームにも必要である。

2. 企業 SOC とサービスプロバイダーは統合 IT/OT ソリューションが必要

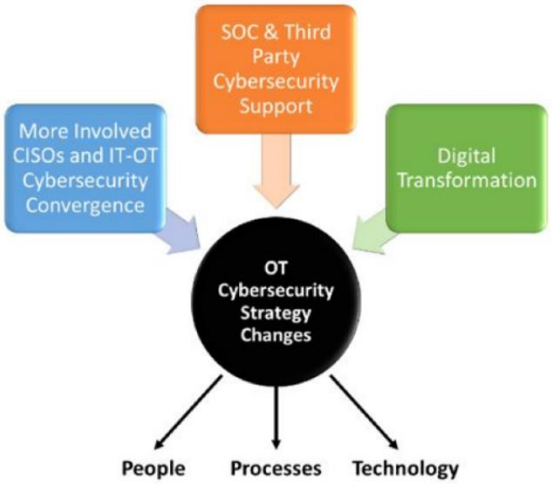
サイバーセキュリティマネジメントは、産業/OT セキュリティリーダーにとって継続的な課題です。殆どの企業内スタッフは、セキュリティの更新とかシステムアラートを把握する時間やこの分野の専門知識が不足している。限られた予算と OT サイバーセキュリティ人材の不足により、OT セキュリティマネージャーは、ユーザサポートに向けた SOC とか MSSP を活用する必要に迫られている。

3. デジタル化により OT セキュリティのモニタリングが必須になる

産業系企業は、継続的にコストを削減し、パフォーマンスを向上させるよう努めている。そのため、こうした多くの企業はデジタルトランスフォーメーションの対策を立ち上げて、運用に必要な詳細情報の入手に取り組み始めている。こうした対策の取組みには、OT システムとエンタープライズアプリおよびクラウドアプリとの接続、および OT システム内での IoT デバイスのサイバー脅威も含まれている。

こうした対策の中で、継続的な OT ネットワークモニタリングソリューションの新しい要件が策定される。IoT のような新しいデバイスが拡大すると、OT でサイバーセキュリティ対策をサポートするためにスケーラビリティが大幅に必要になってくる。新しい IoT デバイスは、OT 環境では一般的に見られないような独自 OS とか通信プロトコルをサポートするような DPI も必要となる。

複雑なアーキテクチャと新しいネットワークアプライアンスでは、小規模ネットワーク用のアプライアンス、アクティブコレクター、仮想型コレクター、スマートスイッチやエッジゲートウェイに組み込み可能なコンテナー型ソリューションなど、柔軟なモニタリングオプションが必要となる。



（注）IT/OT の統合、企業 SOC およびサードパーティサポートの活用、デジタル化の急速な業界の変化には、継続的な OT モニタリングを含む新しいサイバーセキュリティ戦略が必要となる

4．Nozomi Networks は新しい市場ニーズにどう対処するのか？

Nozomi Networks の OT および IoT の見える化をサポートするセキュリティプラットフォームとして、Nozomi Guardian、Remote Collector、および Central Management Console（CMC）の以下の主要コンポーネントを製品ファミリとして用意している。

- **Nozomi Guardian:** この製品は、ネットワークモニタリングのメインの役割を実行する。そして、メッセージ解析、DPI、資産検出、脅威検出、および異常検出の機能が含まれている。また、ネットワークの見える化、脆弱性評価、リスク監視、セキュリティレポートをサポートする。
- **Remote Collectors:** Nozomi Guardian は、リモートコレクターを通じてネットワークトラフィック情報を取得する。リモートコレクターは、制御システムネットワークからパッシブでメッセージを抽出する。Nozomi Networks は、アプライア

ンスおよび仮想タイプのリモートコレクター製品と、アクティブスキャンオプションであるスマートポーリングを提供する。

- **Central Management Console:** CMC は、複数の Nozomi Guardian から収集データを集約し、一元的にサイバーセキュリティマネジメントを可能にする。Nozomi Networks によると、中央管理コンソール（CMC）は数千の Nozomi Guardian サイトをサポート出来る。また、MSSP とか大規模なエンタープライズ向けのマルチテナンシーソリューションとして使用することも出来る。

Nozomi Networks の継続的な OT ネットワーク見える化プラットフォームは、上記で記述した 3 つの市場の変化すべてをサポートしている。見える化と統合性は、常に重要なフォーカスポイントである。色々な OT 製品、ネットワークデバイス、SIEM、一般的な IT セキュリティ管理ツール、アクセス制御製品のインターフェイス、および外部アプリケーションとデータを共有するためのオープン API を備えている。その他最新の機能強化により、企業は、重要なネットワークインフラを中断することなく、OT および IoT 資産の安全なセキュリティ対策を実現する。

終わりに、

OT サイバーソリューションは今後、上述したビジネスニーズへの対応は不可欠である。多くの Nozomi ユーザは、継続的な OT ネットワークモニタリングによって最新の資産インベントリと異常検出の恩恵を既に受けている。見える化とセキュリティソリューションがアクティブスキャン、コンプライアンスサポート、SOC および IT アプリケーションとの統合、そして高度なアラートフィルタリング、IoT デバイスのサポート等といったトレンド対応の新しい機能が期待される。

IT/OT 統合、サードパーティのセキュリティサポートそしてデジタル化の波は、あらゆるビジネスにインパクトを与え、色々な方法で自動化システムを使用するようになる。急速に変化する世界で、我々は OT 運用オペレータに Nozomi Networks の評価を進め、セキュリティソリューションプロバイダーが今後の市場ニーズに対してどのようにサポートすべきかを積極的に検討することを期待したい（筆者）。