NOZOMI NETWORKS

<ホワイトペーパ抄訳版>

Transportation:

OT/IoT の見える化とセキュリティ対策の取組み

September 2020

株式会社テリロジー

1. はじめに

OT/IoT の見える化とセキュリティインシデント

トランスポーテーション（輸送）& ロジスティックス（物流）業界は、サービスレベルと効率の改善の自動化が急速に進んでいます。そして、サイバー脅威のリスクが高まるにつれ、安全性がこれまで以上に重要課題になっています。2020 年の世界経済フォーラムでは、世界で 5 番目に高いリスクとして、トランスポーテーション（輸送）を含む社会重要インフラへのサイバー攻撃を取り上げています。

ITS(Intelligent Transport Systems：高度道路交通システム)は、DX 化により高度で複雑なネットワーク接続化が進み、OT/IoT/IT 全体でネットワークと資産の見える化の必要性が高まっています。

Good News として、リアルタイムによる OT/IoT 見える化ソリューションをうまく活用して、ITS の見える化とサイバー攻撃に対する復旧力(resiliency)の両面を向上させ、ITS に向けた安心・安全性を確保が推進し始めています。

輸送 & 物流システムで使用されるデバイスコンポーネントは DX 化され、ネットワークにフル接続されています。道路センサーと LIDAR（ライダー）を備えた交通管制システム(TCCS)から、トンネルの照明・空調システム、鉄道の電力制御システムまで ITS ネットワークと関連資産の数は急速に増大しています。 そして、多くの IT 管理者にとって、各種輸送システムは**“ブラックボックス”**であり、現実的に、ネットワーク、資産そして脆弱性の見える化は難しい状況です。又、従来の IT ツールでは、OT/IoT デバイスとネットワークのモニタリング機能が不足しています。

（注）：LiDAR（ライダー）は、レーザー光を使ったセンサの一種で、対象物までの距離はもちろん、位置や形状まで正確に検知できることが特徴で、市街地における自動運転には LiDAR（ライダー）が必要不可欠と言われるほどの技術です。

セキュリティ運用対策への道

このホワイトペーパでは、ITS ネットワークのモニタリングおよび脅威検出の統合化ソリューションにより、これらシステムの可用性、見える化、およびセキュリティを容易に実現できる方法を解説します。

こうした ITS システムのネットワーク接続の普及によって、多くの脆弱性を狙った攻撃対象領域(Attack surface)が広がっています。例えば、**NotPetya** のランサムウェアが海運業および物流の世界的企業**“Maersk 社”**を攻撃するのに使用されました。

これは偶発的に起きた訳ではなく、この攻撃のターゲットになった Maersk 社は 2 週間の操業停止で、ロサンゼルス港湾最大の貨物ターミナルの閉鎖と **3 億ドル**の損失被害が報告されました。

このようなインシデントに対して、公共および民間の輸送システム企業の CISO や運用管理者は OT サイバーセキュリティ脅威に警戒し始めました。これら業界のリーダには、企業全体のサイバーリスクの軽減対策が余儀なくされています。これには、企業の ITS が含まれます。その結果、OT/IoT ネットワークの見える化とサイバーセキュリティ防御の改善対策が現在取られるようになりました。その結果、幅広い包括的なセキュリティソリューションが必要になります。サイバーセキュリティスキルの高い IT エキスパートは、ITS を保護するという課題に注目し始めています。　Nozomi Networks の OT/IoT セキュリティソリューションは、世界中の主要な輸送システム分野で安全性が実証されています。

2. 輸送システムの安心・安全性確保の課題

2.1 空港

空港は最も複雑な生態系の 1 つであり、色々な Stakeholders（乗客、サプライヤー、サービスプロバイダー）とテクノロジーの課題が存在します。これらは DX デバイスによって制御されますが、COVID-19 の対策も考慮する必要があります。機能別にサイロ化された設備制御システムは相互に接続されており、その中でもスキャナー、アクセス制御システム、セキュリティ監視カメラといったデバイスに多くの IoT センサーが使用されています。

それと 同時に、空港管理者はサイバー脅威の拡大に懸念を抱いています。サイバー犯罪者は、ランサムウェアを使用して、多くの空港施設を管理している設備環境に攻撃を仕掛けています。2019 年、米国ニューオーリンズ市は非常事態を宣言するほどの深刻なサイバー攻撃の被害を受けました。今回、ニューオーリンズ国際空港のオペレーションには殆ど影響はありませんでしたが、空港の管理責任者は、ランサムウェアや潜在的なハッキング攻撃者や他国からの攻撃に対するサイバーリスク評価対策を織り込む必要があると云っています。以前、この空港は物理的な安全対策に依存していましたが、現在、色々な設備デバイス相互のネットワーク接続の拡大により、サイバーセキュリティに関し空港インフラ全体の重要なセキュリティ対策として取り組んでいます。

空港で直面している課題

空港の運用管理者は、エンドツーエンドのセキュリティを強化するという大きなプレッシャーに直面しています。

空港設備のセキュリティ対策を改善するための主要な課題は、サイロ化されたレガシー制御システム、色々なデバイス相互間の接続が複雑すぎること、および急速に洗練化しているサイバー脅威です。

最初のステップは、使用中全ての OT および IoT デバイス、ネットワーク、および各種制御システムを見える化することです。これが達成されると、ベストプラクティスとリアルタイムでの異常検知および脅威性をモニタリングすることで、サイバーセキュリティ、安全性、および運用の復旧力を大幅に向上させることが出来ます。

2.2 バス、鉄道、高速道路

バス、鉄道、そして高速道路の運用管理システムは、社会基盤にとって不可欠な重要インフラの１つと見なされています。
交通機関の信号制御システムが一旦、中断されると、都市や地域全体が混乱に陥る可能性があります。これらの公共機関では、テクノロジー、IoT センサー、接続性を活用して交通インフラの利用方法が進み、乗客の安心・安全が向上しています。

ITS の運用復旧力の課題に目を向けるということは、一般的にサイロ化されたこの分野の IT と OT 分野の課題解決ニーズを満たすことを意味します。交通システムの IT 運用チームは、ITS の資産、通信、およびネットワークをモニタリングし、システムの脆弱性を評価したいと云っています。
見える化が達成されると、彼らはサイバー脅威を分析し、脆弱性を減らすためのアップデートが講じられているかどうかを確認します。一方、OT 運用チームは、可用性と安全性について懸念しています。彼らは、サイバーインシデントが通常の OT 運用に影響を及ぼしたり、他に影響を与える可能性がないかどうかを把握する必要があります。又、悪意のあるサイバー攻撃は、インシデントだけでなく、人的な操作ミスの可能性もあります。

例えば、資産のコンフィグ設定ミス、機器の故障につながる　不十分なソフトウェアバージョンの管理、フィールドデバイスにつながるワイヤレス接続の不備等です。
このような状況を早期に警告することで、運用管理者は、ダウンタイムが発生する前、または安全性が脅かされる前に事前に対応することが出来ます。

IT/OT の分離を橋渡し

IT と OT 別々に引き起こされるサイバーセキュリティの死角を減らすには、リーダーシップと適切なツールが必要です。

Nozomi Networks ソリューションは OT の安全を目指し、可用化を向上させます。又、既存システムやワークフローを統合させながら、IT に必要な可視化とサイバー脅威の検出も提供します。

世界中の輸送システム管理者はモニタリングを実施していますが、残念ながら、ITS のサイバーリスクと運用上のリスクレベルの見える化の欠如が露呈しています。安全性と収益を確保する必要性の懸念が高まる中、多くの公共および民間の交通システムで ITS の見える化とセキュリティソリューションに投資しています。

2.3 海運

海運産業は世界貿易の 90%が輸送業分野で他の産業同様、ネットワーク接続、自動化そして、リモートでのモニタリングが推進されています。船荷主は、航海を最適化し、次のようなことをモニタリングしたいと考えています：

- ☐船舶の積載状況
- ☐燃費
- ☐位置とルート（航路）
- ☐機関性能
- ☐システム効率

一方、海運システムの見える化レベルとサイバーセキュリティ対策は他業界と比較するとまだまだ低いのが現状です。
多くの船舶には、運行管理者が気づいていない設備デバイスと制御システムが含まれているようです。乗組員は通常、フィッシングメールを識別したりネットワークアクセスのセキュリティ管理をしたりする訓練を受けていません。船舶がハッキングによって転覆するような劇的な状況は、可能性の想定外ではありません、
乗組員は常に船舶の予兆（予知保全）をチェックし、異常な予期しない性能変動を検知した場合、手動または安全システム(SIS)を活用して修復することがよくあります:
急速な DX 化は海運自律システム（MAS）の改善も実施しており、陸上とのリモート通信の制御も行われています。

想定外の攻撃は、資産管理者にとってコストがかかる可能性があります

サイバー攻撃者は、海運システム運用管理者に対して、ランサムイウエア攻撃で彼らの運行制御システムを停止させて、復旧に向けた費用（身代金）を要求します。

eMail フィッシングにより、コンテナ船海運最大手 Maersk 社は NotPetya ランサムウェアに感染。その被害状況には、4,000 サーバと 45,000 台の PC のネットワークの再構築が含まれています。

インシデントリスクの高い破壊的なイベントには、次のものがあります：

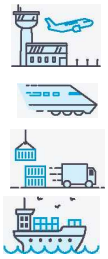
- ☐意図せずに引き起こされる運用システムの信頼性を脅かすようなサイバーインシデント
- ☐企業の出荷ワークフローを妨害したり、ドキュメントを改ざんしてドラッグの密輸を促進するようなサイバー犯罪者
- ☐港湾での積載クレーン操作とか積載商品のフロー処理を停止させるような船舶から陸上への陸揚げ機能を停止させる脅威

海運会社は、サイバーリスクの軽減対策や、サイバー被害の防止対応に投資しています。重要な対策課題は、海事資産と通信プロトコルを正確に識別することです。ネットワークは、サイバー攻撃の可能性のある脆弱性、脅威、および異常な振舞いがないかモニタリングする必要があります。

3. Nozomi Networks Solution

3.1 Nozomi ソリューションは運用復旧力とサイバー攻撃防御をどのように対応するか?

Nozomi Networks は、輸送システム担当の資産運用管理者が DX 化を加速するのを支援します。Nozomi ソリューションは、OT、IoT、IT、サイバーフィジカルシステム全体の見える化と脅威検出を統合します。
そして、Nozomi Networks は、企業の ITS ネットワークへのサイバー攻撃リスク削減対策に貢献します。



Nozomi Networks

Nozomi Guardian の導入により輸送業界に従事している何十億人もの関係者をセーフガードします。

Nozomi Networks は、ITS の見える化、脅威検出、その他サイバー脅威を世界中の大手企業に提供します。
AI/ML の革新的なテクノロジーを通じ、Nozomi ソリューションは、ITS ネットワークの資産とネットワークのモニタリングを自動化します。
資産運用管理者は、サイバー攻撃による復旧力と信頼性を確保するため必要なリアルタイムでの見える化と脅威検出の恩恵を受けます。

Guardian

Nozomi Guardian は、OT/IoT セキュリティと見える化機能を提供します。資産のデスカバリー、ネットワークの見え化、脆弱性評価、リスク評価そして脅威検出機能を 1 つのソリューションに統合します。スマートポーリングアドオン機能は Passive なアセットデスカバリーを拡張し、Active ポーリングでアセットの詳細なトラッキングを可能にします。

Central Management Console(CMC)

中央管理コンソール（CMC）は、OT/IoT のリスク評価と、エッジまたはクラウドの分散サイトの見える化を一元化します。IT セキュリティインフラと統合して、ワークフローを合理化し、脅威や異常検出を迅速にサポートします。

Threat Intelligence

脅威インテリジェンスサービスは、継続的な OT/IoT の脅威および脆弱性インテリジェンスを提供します。
これにより、ダイナミックに脅威状況を把握し、平均検出時間（MTTD）の工数を改善します。

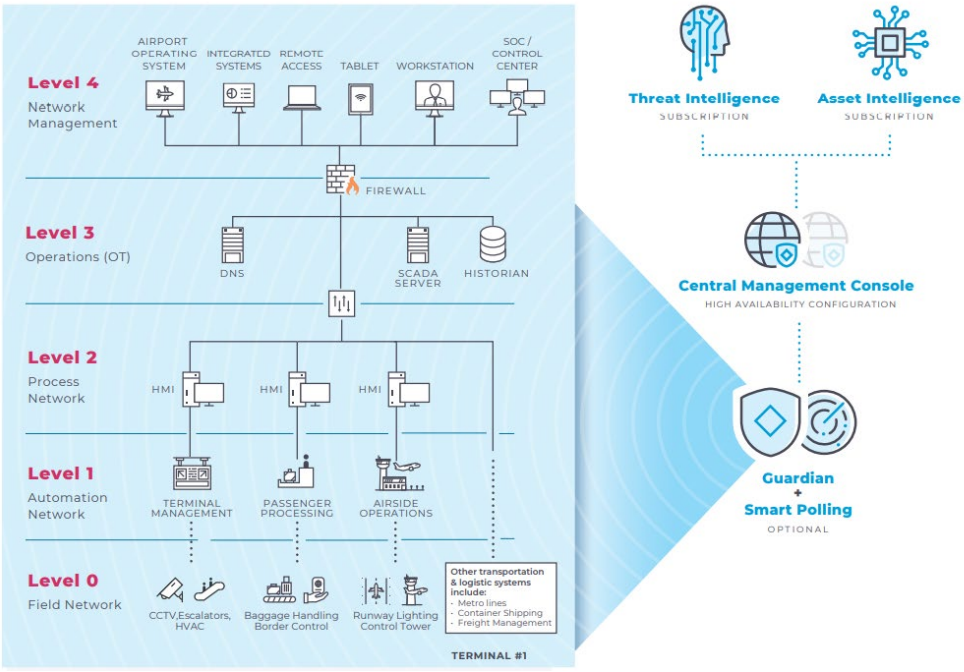
Asset Intelligence

アセットインテリジェンスサービスは、継続的な OT/IoT アセットインテリジェンスを提供して、より高速で正確な異常検出を実現します。それは運用管理者の平均応答時間（MTTR）の工数削減を支援します。

3.2 Diagram: OT/IoT Security と見える化

以下に示すのは、Nozomi Networks ソリューションをデプロイして、空港の運営に関係する多くのシステムの見える化とセキュリティ強化を提供するユーザ例です。（他の運輸部門でも同様の図が利用出来ます。）

Deployment Architecture: パデューモデル例



4. ネットワーク運用の見える化の向上

4.1 ユーザ事例: マルチシステムオペレーションの見える化を高める

この分野の複雑な環境により、統合された OT/IoT の見える化が非常に困難になります。これによって又、攻撃対象領域が拡大し、サイバー脅威に対する脆弱性を増大させます。管理作業をスムーズに行うために、運用管理者は、IT/OT 環境の様々なデバイスの資産管理方法と、全ての ITS ネットワークに関わる詳細デバイスのモニタリングが必要になります。Nozomi ソリューションは、空港、鉄道、地下鉄、その他輸送管理システムで見られる複雑な運用管理の課題解決に対処します。

Nozomi ソリューションがデプロイされると、ITS 資産の正確で一元化されたインベントリーが自動的に作成され、これら最新状態を確認することが可能になります。 これにより、詳細なアセットビューのドリルダウンが容易になります。

☐ITS 全体の Macro View 機能。サブネットとネットワークセグメント毎のフィルタリング機能。

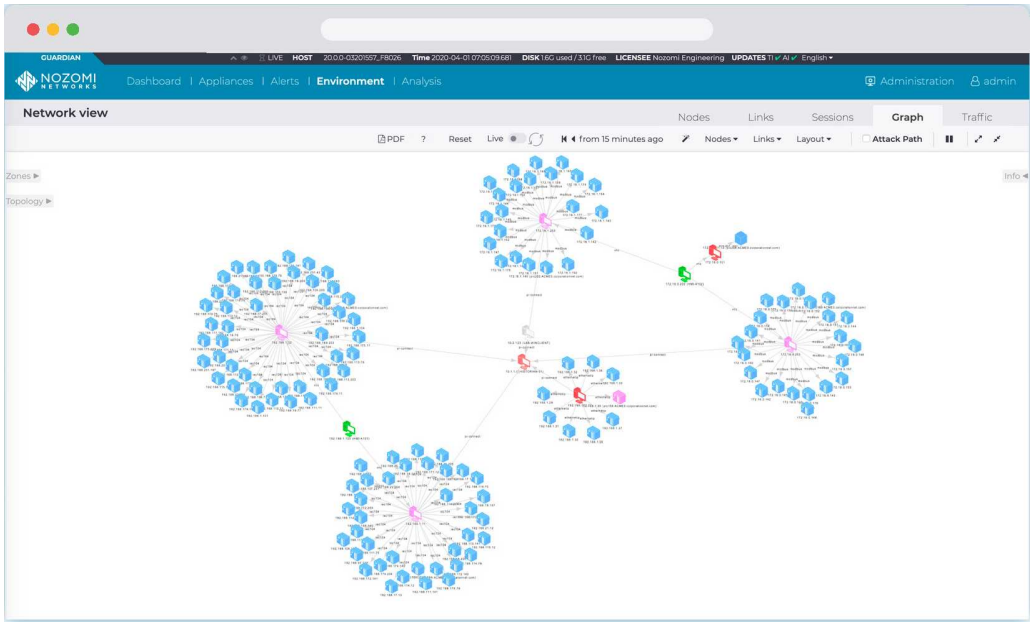
☐各ノードの役割とノード間のトラフィック情報。

☐ノードとゾーン間の通信に使用される制御プロトコル。

☐スループット、制御プロトコル、オープン TCP 接続などのネットワークトラフィック情報。

☐エンドポイントとの接続に関する詳細な属性。

Nozomi ソリューションは、OT/IoT の資産とネットワークの見える化向上を促進します。取得情報のカバー範囲は、これまで把握出来なかったデバイス、相互接続、およびアクティビティに関する深掘りになります。



Nozomi Networks Solution: Network Visualization Graph

Nozomi Guardian のデプロイから数分以内に、運用ネットワークの資産インベントリーが作成され、多くの場合、これまで把握出来なかったデバイス、相互接続、およびアクティビティが明らかになります。

4.2 ユーザ事例: 運用の中断とダウンタイムの防止

世界経済は、人とモノのシームレスなやり取りにより進展しており、その中で貨物船舶は、1 回の航海で 8,000 個のコンテナを輸送しています。

そして、輸送システムは毎年 530 億人以上の乗客を運び、88 億人以上の乗客が世界中の空港を利用しています。

こうしたシステムの停止やテクノロジーの不具合が利用者や業務プロセスに与える影響について考えてみて下さい。乗り継ぎの失敗、手荷物の遅延といった日常の不具合な状況は、全体から見ればほんの一部の影響かもしれませんが、ただこうした想定外のダウンタイムは、複数の拡大要因に影響します。例えば、24 時間年中無休で稼働中のデバイスが動作しなくなったり、ネットワークの設定変更によって OT システムが障害を起こしたり、サイバーインシデントによって重要な運用プロセスが停止したりします。

毎分という時間の単位の重要な輸送業務の中で、運用管理者は、発生する問題を見つけ、それに対応するために貴重な業務時間を失う可能性が出てきます。

空港で PLC に障害が発生し、手荷物処理システムが機能しなくなったケースがあり、そのために、長時間の停止が発生しました。

潜在的な機器デバイスの予兆を事前に特定し、サイバー脅威によって運用業務が中断する前に、事前に発見することのメリットを想像してみてください。

Nozomi ソリューションは、Passive なネットワークモニタリングと異常検出機能を使用して障害のある機器を素早く特定し、輸送システムのダウンタイムのリスクを大幅に削減します。

ベースライン化

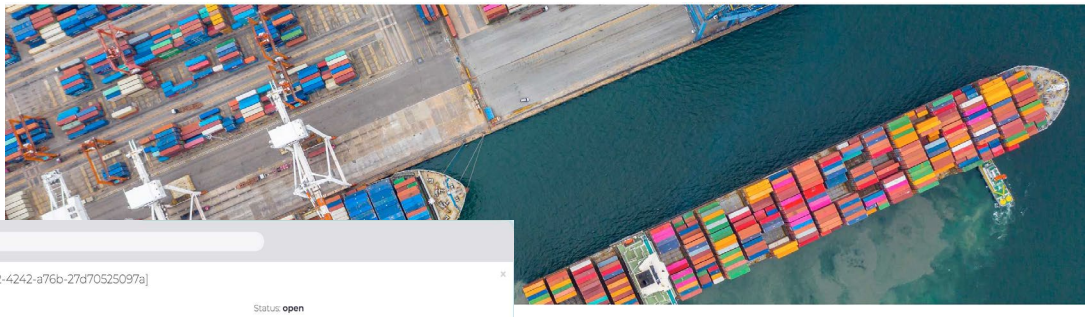
Dynamic Learning の初期フェーズで、Nozomi ソクソリューションは、AI/ML を活用してネットワークトラフィックをモニタリングし、ベースラインを作成します。

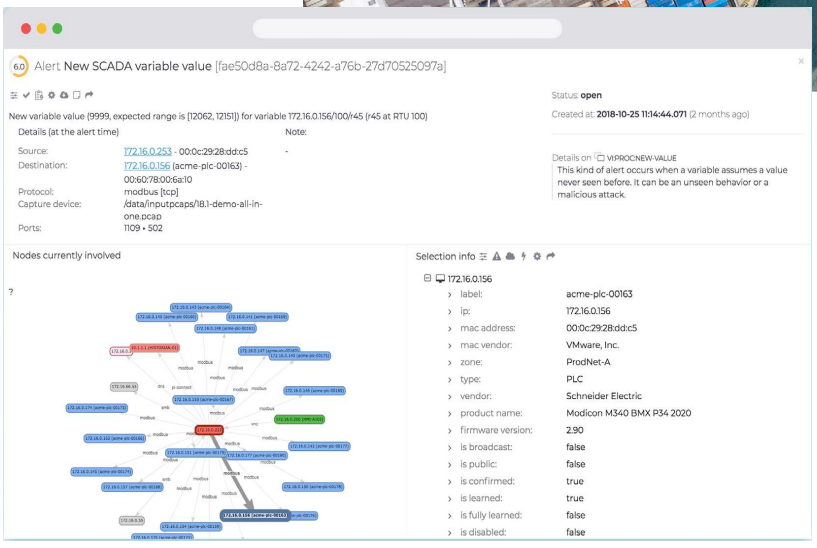
システム内の資産情報を含むデータを相連付けて資産状況をモデル化し、正常状態を自動設定します。

異常状態の検出

モニタリングフェーズで、Nozomi ソリューションは、特定デバイスまたは自動化されたオペレーションがベースラインから逸脱し、サービスを中断する可能性のある状態を自動的に検出します。マルチベンダー、マルチプロトコルネットワークで何が起こっているかの状態を統合された分かり易いビュー表示して、修復が必要になる場合、事前に警告します。

Nozomi の Networks Asset Intelligence と組み合わせた異常検出により、トラブルシューティングの労力が大幅に削減され、デバイスまたは自動オペレーションが不能になる前に対応します。





5.サイバーリスクの検出とサイバー回復力の向上

5.1 Use Case: システムの脆弱性がどこにあるかを把握する

輸送運用システムには、複数ベンダーのデバイスで構成されています。残念ながら、殆どの運用制御デバイスには、乗客、諸元データ、および運用システムを安全に維持するために必要十分なセキュリティ機能は殆ど備わっていません。多くの OT/IoT 環境には、IT アプリケーションとか IT システムで採用されているような認証や暗号化技術といったセキュリティ対策は徹底されていません。

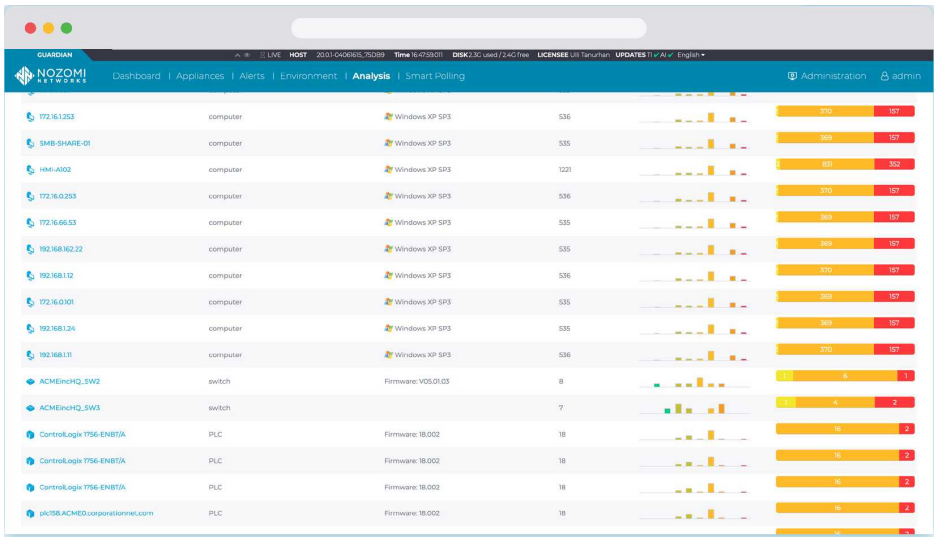
Nozomi ソリューションは、運用システムの脆弱性を自動で評価することにより、この課題を解決します。

ウイークポイントを明確にし、重要な脆弱な露出ポイントを優先し、デバイスが悪用される前に事前に対処します。

この Nozomi ソリューションは、次の要件を満たします:

- ☐ベンダーX のデバイスは脆弱ですか？
- ☐WindowsXP のアセットはいくつありますか？
- ☐脆弱な特定デバイスを更新する必要がありますか？

セキュリティチームが脆弱レベルの高い露出ポイントに優先付けし、デバイスベンダー毎に脆弱性スコアが専用ビューに表示されます。 更に、脆弱性のドリルダウンによって、トラブルシューティングと修復を支援します。



Nozomi ソリューション: 脆弱性リスト

脆弱性の自動評価機能は、どのエンドデバイスがリスクに晒されているかを迅速に特定し、修復作業を最優先事項としてフォーカスします。

5.2 Use Case: OT/IoT ネットワークに影響を与える前にマルウェアを検出する

2008 年、ポーランドの **Lodz** に住む 10 代の若者は鉄道ネットワークの脆弱リスクを研究。彼は、テレビのリモコンを改造し、市内の“ライトレール”(Light rail：路面電車)の線路ポイントを管理している運行制御システムにリモート侵入して攻撃。その結果、4 本の路面列車が脱線し 12 人が負傷しました。

このタイプの攻撃は何故これほどの惨事に至ったのでしょうか？

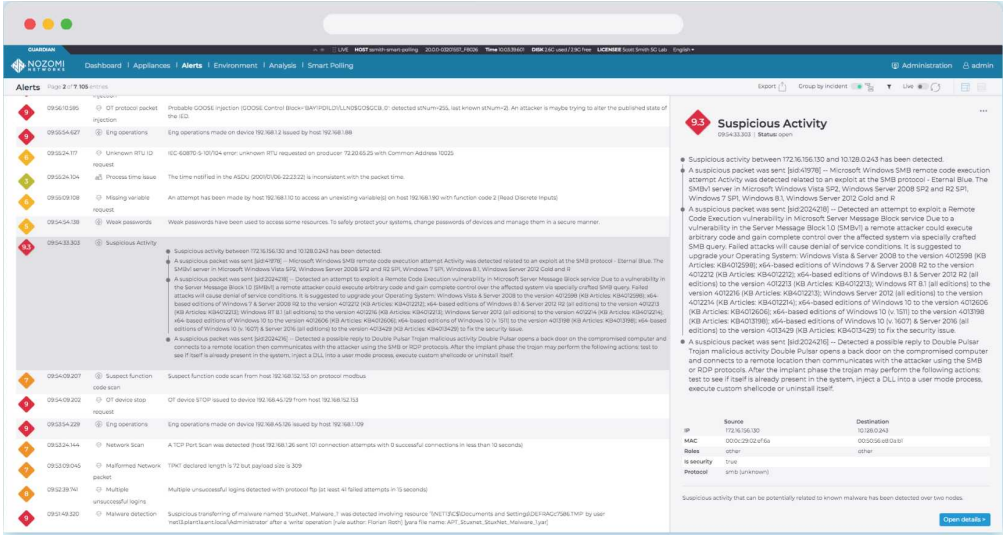
輸送業界での運用システム環境は、不正侵入に対してきわめて脆弱な状態になっています。施設管理、荷役、自動運賃制御、CCTV インフラ、その他運用システムの OT/IoT デバイスには残念ながらセキュリティ機能は備わっていません。これらのデバイスへのサイバー攻撃は、空港や地下鉄を利用する何百万人もの乗客の安全を危険にさらす可能性があります。又、最悪世界中の物流を止めてしまう恐れがあります。交通管理制御サービスは、最終的に攻撃侵入ターゲットが IT ネットワークエントリーポイントにもなってしまいます。

洗練された凶悪なマルウェアは、攻撃中に様々なフェーズの攻撃を仕掛けます。マルウェアが IT と OT のネットワークセグメントで攻撃のダメージを目す前に、そのマルウェアを無力化し、マルウェアを事前にかつ早期に特定することが不可欠です。

Nozomi ソリューションは、ビヘイビアベースの異常検出、シグネチャおよびルールベースを組み合わせたハイブリッドな検出機能を使用して、各攻撃フェーズでのマルウェアを検出します。

- □初期フェーズでは、Guardian の異常検出は、外部の C&C サーバにビーコンを送信しているマルウェアの不規則な振舞いにフラッグを立て、マルウェアのネットワークトラフィックのフローを検出します。
- □偵察フェーズでは、マルウェアは学習プロセスをトリガーにすることで攻撃に備えます。運行システムで、マルウェアが独自の制御システムプロトコルを使用して通信している場合でも、メッセージは通常のベースラインビヘイビアとは異なり、Guardian がそれらを特定することが出来ます。
- □ Guardian を使用すると、初期フェーズと偵察フェーズの両方の攻撃で、輸送事業者が新しいファイアウォールルールを実装して通信をブロックしたりして更なる攻撃コマンドを停止し、被害を最小限に食い止めます。

SIEM などのツールとの統合 API が組み込まれているため、IT スタッフは既存ツールとワークフローを共有して OT の脅威に対してコスト効率よく対応出来ます。Asset Intelligence および Threat Intelligence は、Guardian アプライアンスを継続的に更新し、サイバー脅威や異常発生の前に迅速に事前検出して対応します。



6. おわりに

輸送分野の ITS ネットワークの見える化は運用の修復に役立ちます

輸送システムの運用管理者は、運用効率を高めるために必要なツールとテクノロジーを採用していますが、デジタル化と多様なネットワークの接続性により、リスクが高まり、脅威レベルが拡大します。 こういったサイバー攻撃リスクにより、運用の中断による迅速な対応とか、サイバー脅威を回避することが困難になると予想されます。

グローバルな輸送業者の保護

これには、OT/IoT の見える化と脅威予知の検出が不可欠です。これが出来ないと、ITS ネットワークで何が起こっているかを把握出来ません。ネットワーク上の脅威の問題は、安全性、システム稼働時間、事業収益、乗客/旅行者の心理的なプロセスに大きな影響を及ぼす可能性があります。信頼性を脅かす問題の検知とトラブルシューティングには、リアルタイムでの見える化が必要です。残念ながら、多くの資産運用管理者は、デバイス、接続、および通信に関する目線を欠いています。こうした人、プロセス、テクノロジーに関連するセキュリティギャップは、運用の修復力にも大きな影響を及ぼす可能性があります。例えば、IT と OT は、接続されている ITS 制御システムと組み合わされて、死角によって脆弱性につながる危険性があります。しかし、適切なテクノロジーとベストプラクティスに重点を置くことで、輸送事業者は運用の修復力を高めることが出来ます。Nozomi ソリューションを使用すると、見える化とサイバーセキュリティ防御を容易に実現出来ます。 このソリューションは、制御ネットワーク上のすべての資産の最新状況を自動的に表示出来、ITS の見える化が可能です。次に、異常に関してネットワークビヘイビアをモニタリングし、潜在的な予兆変化を示す可能性があれば、運用管理者にアラートします。このソリューションは、高度な脆弱性と脅威検出の機能に加えて、より迅速な優先付けと修復につながる詳細な洞察も提供します。Nozomi ソリューションは、輸送事業者の固有の課題に対応するように考慮されており、セキュリティおよび運用チームが ITS 制御ネットワークを見える化するのに役立ちます。 これは、運用システムのダウンタイムの防止、脆弱性レベルの把握、マルウェアの検出、インシデント対応に大きく役立ちます。

7. カスタマーレビュー

以下の顧客は Nozomi Networks にトップスコアを与えます

★★★★★

Exceeded Expectations. Deeper Visibility Than Expected.

我々は、全てのベンダーが“Cookie-cutter（独自性に欠ける）”ソリューションのように感じました。ただ、Nozomi Networks だけは違っていました。Nozomi Networks を導入して、彼らの解決提案はその通りでした。我々の選択は正しかった。

某企業 Senior Industrial Security Manager ›

Once You Try Nozomi And Its Rich Feature Set You Cannot Imagine Operating Without It!

Nozomi プラットフォームは他の競合製品と真っ向から対峙し、テスト時に市場に出回っている他のどのツールよりも多くの L2 デバイスを見える化して適切に分類することが出来ました。

某企業 Security Analyst ›

Great Solutions For ICS.

このソリューションには、インベントリーや脆弱性分析機能など、OT 環境を管理する多くの機能があります。 このソリューションは更に、ニューラルネットワークの通信フローマップがあり、インシデント対応に非常に関連性のある情報が含まれています。

某企業 IT Analyst ›

あとがき：

本ホワイトペーパ抄訳版は Nozomi Network から提供されたブログをベースに不必要な部分は省略し、更に筆者が追加した資料です。Nozomi Networks の Guardian 製品はヨーロッパ、中東地区で大手鉄道や地下鉄等の分野で導入が始まっています。この Transportation 分野は日本国内では社会重要インフラにリストアップされており、今後多くの乗客と貨物の輸送システムのリスク管理とアセスメントが重要になると予想されます。

出典

INDUSTRY BRIEF

Transportation:

Improving Operational Resiliency Through OT and IoT Visibility and Security

September 2020

関連リンク

https://www.nozominetworks.com/

お問い合わせ窓口

株式会社テリロジー OT/IoT セキュリティ事業推進部

Nozomi Networks Guardian 担当 宛

製品に関するお問い合わせは当社のお問い合わせフォームからお寄せください