Nozomi Networks v19.0

ICS セキュリティソリューションの新機能リリース

株式会社テリロジー

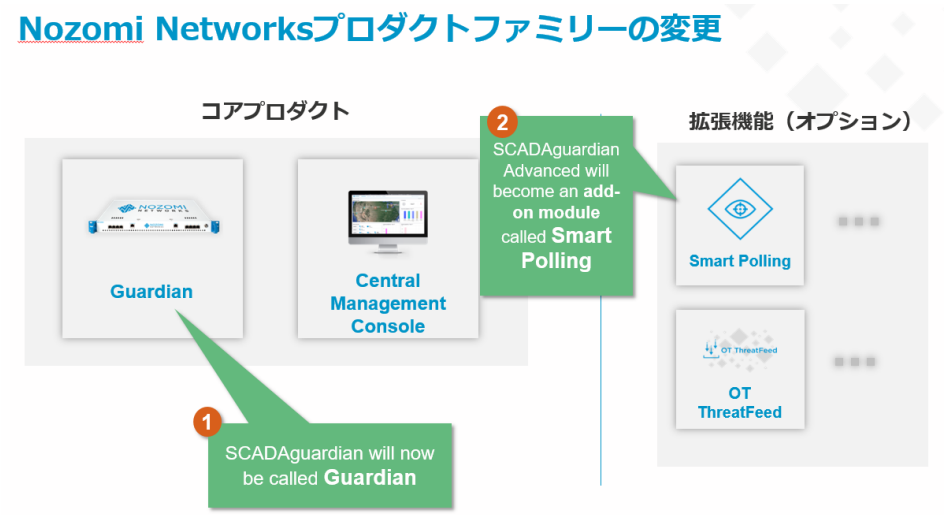
産業制御システムへのサイバー攻撃（Triton、LockerGoga、Industroyer 等）は、世界中で拡大しています。そして、企業内 ICS インフラ（産業制御システム）環境の 3 分の 1 以上が、昨年サイバー攻撃が侵入したかどうかわからないと報告しています。これは OT 環境でのセキュリティ監査（資産の見える化）とサイバー脅威検出の必要性を示唆しています。こうした産業分野のセキュリティ課題を念頭に置いて、Nozomi Networks は v19.0 という新機能をリリースしました。

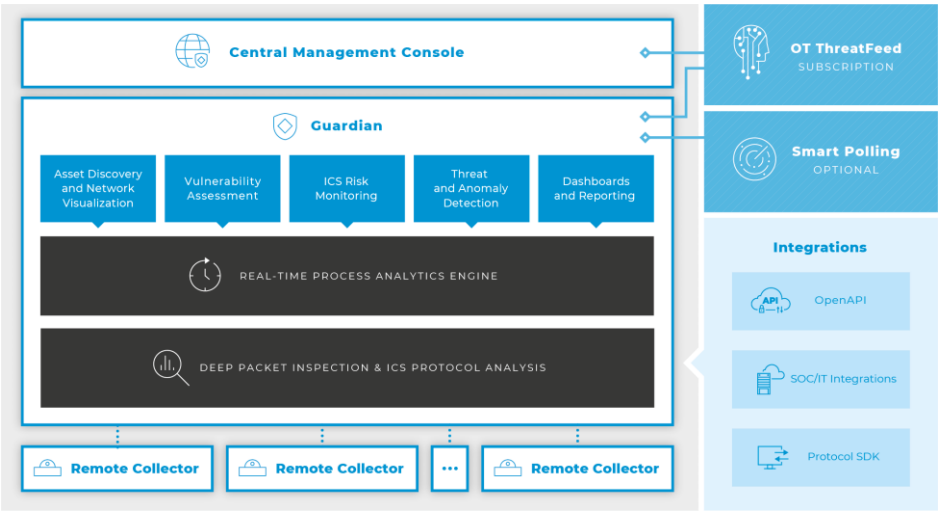
Nozomi Networks では、顧客の ICS インフラ環境の“真の見える化”がサイバーリスクを軽減するための鍵だと考えています。しかし真の見える化は SCADA 環境だけに留まりません 何故なら、それは IT/OT/IoT 相互間のギャップを埋めることが必要だからです。

v19.0 では、ICS の領域を超えて、セキュリティをより包括的かつ効率的な方法で管理する点にフォーカスします。

新しい名称による卓越したソリューション

SCADA システムからスマートシティまで、サイバーセキュリティの必要性はあらゆる環境に広がります。Nozomi Networks のカバーするソリューションは常に SCADA の領域をはるかに超えています。今までの Nozomi Networks の製品名（SCADAGuardian）は必ずしもそのニーズに即していません。ソリューションの領域拡大の適用をよりよく反映するために、Nozomi Networks の主力製品の名前を **Guardian**™に変更しました。





Nozomi Networks v19.0 ソリューションは、新しい製品名とそのスケーラブルなモジュールベースのアーキテクチャーを含んでいます（上図参照）。

同様に、Nozomi Networks はアクティブな資産デスカバリーソリューションを **Smart Polling™**（以前の SCADAguardian Advanced）に改名しました。Smart Polling は、Nozomi Networks の独立した製品ではなく、Guardian のアドオンモジュールとしてオプション利用出来るようになりました。

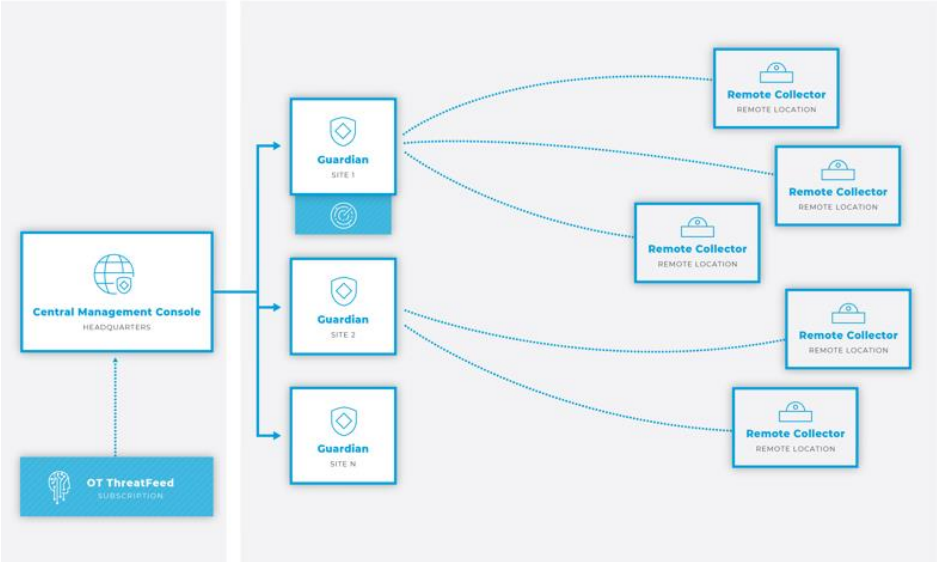
Nozomi Networks プロダクト名は変更されていますが、コアテクノロジーと製品の機能は何ら変わっていません（勿論、v19.0 では追加機能も含まれています）。

v19.0 の新機能と改善点

エンドツーエンドの見える化とサイバーセキュリティに重点を置いて、Nozomi Networks は最新のリリースでかなりの新機能と機能改善を追加しました。v19.0 の新機能を簡単に紹介します：

リモートコレクター(Remote Collector)で適用範囲を広げる

すべての ICS インフラ環境で同じように適用される訳ではありません。特に ICS 施設の拠点ががオフサイトやオフショアにある場合、企業はサイバー脅威に関してこうしたリモート拠点のあらゆる ICS セグメントでも監視する必要があります。Nozomi Networks は v19.0 の機能としてリモートコレクターを追加しました。このツールは顧客管理者が手の届きにくい自社遠隔拠点サイトの資産情報とネットワークデータを収集するための費用対効果の高いコンパクトなデバイスです。リモートコレクターは分析とレポート作成のためにこれら収集データを Guardian に送信します。



簡易型デバイスのリモートコレクターは遠隔拠点のサイトに設置して、ICS インフラへのセキュリティ脅威とネットワークのモニタリングの関連データの収集のみに使用します。

新しいビルトインレポートでコンプライアンスのリスクとセキュリティの状況を把握

今回の v19.0 リリースでは、ICS インフラ環境内のすべてのデータに対してカスタムレポートをすばやく作成して実行出来るようになりました。

そして、v19.0 では、現在のセキュリティ状況を見える化し、コンプライアンスのリスクを把握するのに役立つ新しいビルトインレポートを利用出来るようになります。今後数ヶ月にわたり、Nozomi Networks はもっと多くのレポートサンプルのライブラリを追加する予定です。

新しい2つのビルトインレポートがプロダクトのレポート機能に追加：

- **Asset inventory** – 全体の資産リストと関連情報を表示
- **Center for Internet Security (CIS) Controls** – データ情報をCISコントロールにマッピング

＊**米国CIS Controls**は、情報セキュリティ対策とコントロー ルの優先付けされたベースラインを示したコンセンサスドキュメント

Benefits:

- 環境内の資産のリストをすばやく引き出す
- CISトップ20コンプライアンスを満たすためのリスクを理解

Cisco 製品との連携によるインシデント対応の自動化

サイバー脅威の手口は巧妙になり、急速なペースで IT/OT 環境に侵入します。インシデントレスポンスタイムとその修復までの工数を短縮するために、疑わしいアクセス行為に対するレスポンスアクションを自動化する Cisco ASA および Cisco Firepower Threat Defense（FTD）との統合を追加しました。Cisco 製デバイスを Guardian に接続すると、IT/OT 環境内でアラートに基づく以下のアクションを自動化出来ます：

- 新しいデバイスがネットワークに接続されるのを防ぐ
- ネットワーク上のデバイス間で試みられた新たな接続をブロックする
- ファイアウォールから疑わしいセッションを強制終了する

V19.0 で Nozomi Networks ソリューションと Cisco 製品を統合して簡単にインシデントレスポンスを自動化します。

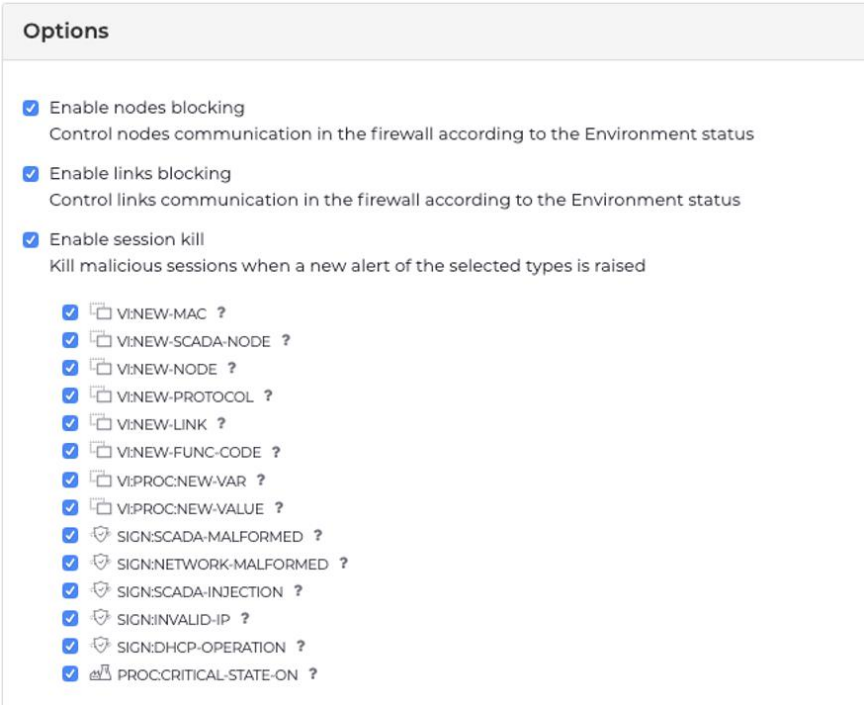
USB Detection for Windows Systems

Guardian オプションの Smart Polling アドオンを使用して、Windows システムで USB デバイスを検出します。

・ICS 環境でインサイダー脅威を検出。

・ユーザが制御システムに外付けデバイスを接続していることをチェック。

Note: 上記の機能には Smart Polling アドオンが必要です。



Aruba Clearpass と Cisco ISE の統合によるアクセス制御の一元化

企業内のサイバーセキュリティに対する最大の脅威は、人的なリソースです。外部者が企業内の ICS システムをターゲットにしていたり、社員による会計処理上の単純なミスを冒したりする“人的な行為”は企業のインフラ環境を守るための最大のリスクになります。Aruba Clearpass と Cisco ISE との統合を通じて、セキュリティチームは、自社のすべての IT および OT ネットワークにわたって完全な見える化とアクセス制御の一元化を実現します。

Windows Data Collection for Smart Polling

SANS 2019 OT/ICS の Cybersecurity は、商用 OS（Windows、Unix、Linux）で稼働しているサーバ資産が、2019 年に ICS インフラにとって最も高いリスクを生み出すと報告。IT 部門の管理者にとって、まだ Windows XP や Windows 2000 で稼働している ICS インフラ環境は悪夢のように思えますが、これらの OS 環境は OT の現場では当たり前のことです。ICS のセキュリティ対策について考える場合、これらの資産デバイスを考慮してリスクと潜在的な攻撃を監視することが重要です。Smart Polling アドオンの v19.0 では、OT 環境内の Windows デバイスから重要なデータを収集出来るようになりました。

・コンピュータシステム情報（ドメイン、プライマリオーナー、物理メモリ、空き容量、ディスクサイズ、パッチ情報、使用されているインタフェイス）

・ユーザアカウント（有効ステータス、ドメイン、フルネーム、ロックアウトステータス、名前、パスワード有効期限）
・インストールされているソフトウェア（ソフトウェア、バージョン、インストール日）使用されているポートとサービス
・有効な USB デバイス情報（USB 名と製造元）
・ウイルス対策ステータス（製品、バージョン、シグネチャ、最終更新日、最終スキャン、実行中のサービス）
・その他

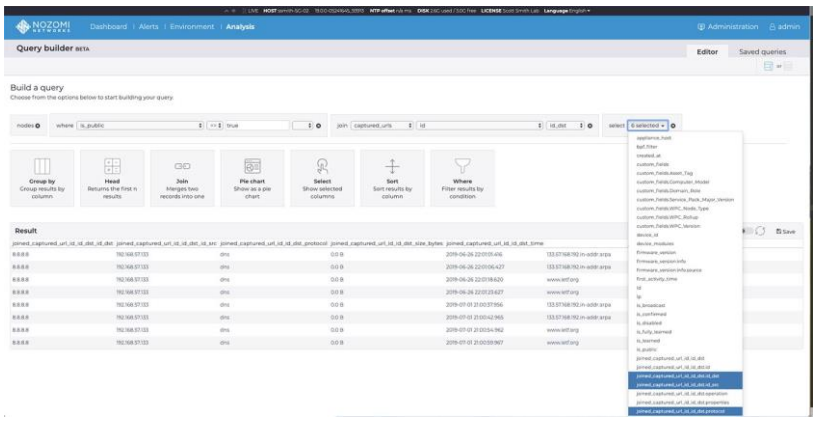
アラートプロファイルの“ノイズ”を削減

多量のアラート処理による負荷は、世界中のセキュリティチームにとって現実の問題です。専門知識に関係なく、アラートが多すぎると、脅威を検出してもタイムリーに対応する能力が低下する可能性があります。v19.0 では、受信したアラートの種類を管理するのに役立つコントロール機能が追加されました。フルカスタマイズ可能な新たな 4 つのビルトインプロファイルを使用すると、どのアラートを表示するか、どのアラートを非表示にするかを決定出来ます。

簡素化されたクエリーを用いて、検索したいものをすばやく見つける

Guardian を最大限に活用するために、新しい Query Builder を用いて、環境内のデータに関するクエリーを簡単に行うことが出来ます。単に見つけるだけでなく、クエリをチャートやグラフに変換して、カスタムダッシュボードやレポートに使用することも出来ます。既存のクエリー構文を使ってもっと複雑なクエリを作成することも出来ます。

Guardian の新しい Query Builder は、レポート作成とダッシュボードの作成を簡素化します。



対応プロトコルの追加

産業分野で使用されている資産デバイスや制御システムを見える化することは容易ではありません。実際、ICS インフラからデータをモニタリングしている企業は 3 分の 1（28%）未満です。TCP/IP で運用する IT インフラを運用している場合と異なり、ICS インフラでは OT ネットワーク全体で何百もの特殊なプロトコルを使用します。これらの OT ネットワークに接続している様々な資産デバイスや ICS を継続的にサポートするために、Nozomi Networks は定期的に新しいプロトコルを追加しています。

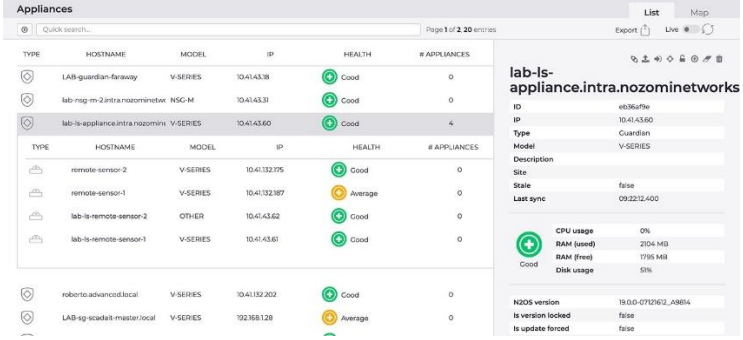
以下は、v19.0 リリースに含まれるもののほんの一部です：

- Wonderware SuiteLink DA
- Weatherford Cygnet
- Mitsubishi Melsoft
- Mitsubishi SLMP
- GE Cimplicity Replica
- GE Cimplicity View
- GE Mark VI
- ABB TotalFlow
- Siemens CAMP
- ZMTP
- Foxboro IA
- OPC-UA

新たな CMC インターフェイスで複数の ICS サイトを一元管理してオーバーヘッドを削減

“Time is money”であり、新しい CMC インタフェイスは ICS インフラのリスクとサイバーセキュリティ管理にベストフォーカスされ、運用管理を簡素化することを最優先としています。そして、CMC のユースケースを増やして、CMC を更に堅牢なセキュリティシステムにするために、今後数回のリリースで更なる改善を計画しています。

改善ベースのロードマップの最初のステップは、ダッシュボードの使いやすさを単純化することです。v19.0 では、デプロイの階層構造と各アプライアンスの正常状態を簡単に確認出来ます。更に、CMC と各アプライアンス間で簡単にアップデート出来ます。



ハイライト:

・改善されたアプライアンス管理インターフェイス

・デプロイメント状況をすばやく把握するための優れた情報提供

・すべてのデプロイメントを迅速にナビゲートするための新しいグループ化機能

メリット:

・すべてのアプライアンスのヘルス状態を簡単に把握

・すべての Nozomi Networks アプライアンスのアップデートを管理

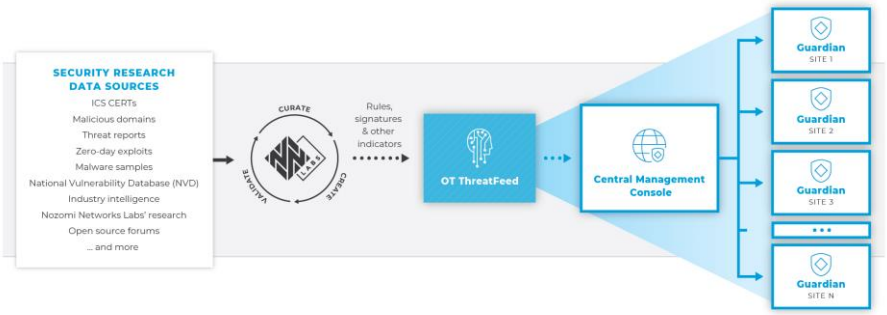
OT ThreatFeed は新たな脅威と ICS ゼロデイを検出する新しいツール

OTT ThreatFeed の機能は技術的な面で v19.0 のリリースとは直接関係ありませんが、OT ThreatFeed は定期的に（1 週間に数回）更新されているので、過去数ヶ月間に起きた脅威のアップデートを把握することは重要です。OT ThreatFeed は、数々のアワードを受賞した実績のある脅威インテリジェンスオプション機能で、ユーザが脆弱性をより的確に特定し、OT 環境内の脅威を検出するのに役立ちます。

ここ数ヶ月の間で、Nozomi Networks Labs のセキュリティ研究者チームは、顧客の ICS インフラで起こっている疑わしい不正行為の新しい脅威を分析し、このツールを開発することに取り組んできました。

- BlackEnergy、DeltaCharlie、LockerGoga、Palevo、Phobos、mashingCoconut などのセキュリティ脅威に対して 800 を超える新しいルール、シグニチャ、および証跡情報を追加
- Nozomi Networks Labs によって発見され、過去 3 ヶ月間に ICS-CERT によって公開された 2 つのゼロデイ脆弱性：
    - Rockwell PLC (ICSA-19-120-01)
    - Mitsubishi PLC (ICSA-19-141-02)

OT ThreatFeed サブスクリプションは、Nozomi Networks Labs の脅威のインテリジェンスで脅威検出を向上させます。



Nozomi Networks 認定エンジニアコースでセキュリティの専門知識を向上

2019 年内に、3 分の 1 の企業が、IT、OT、およびハイブリッド IT / OT 要員のためのサイバーセキュリティ教育およびトレーニングへの参加を計画しています。Nozomi Networks 認定エンジニアトレーニングコースは、IT および OT 運用担当者のためのサイバーセキュリティ知識の向上に向けたものです。Nozomi Networks は、過去数ヶ月にわたり、顧客サイトで 3 日間のインストラクター養成プログラムの Nozomi Networks 認定エンジニアトレーニングコースを開催してきました。このコースは、Nozomi Networks のソリューションを活用して高レベルの ICS サイバーセキュリティとオペレーショナルインテリジェンスを実現するのに役立つように設計された多数の実践シナリオで構成されています。

v19.0 の 2-Step Update Path

v19.0 では、アップデートパッケージのセキュリティ機能が更新され、アップデートがより簡単になります。v19.0 にアップグレードするには、2 段階のアップデートパスの処理が必要です：

・Customer must update their appliance to v18.5.9

・Once on v18.5.9, the customer can update on v19.0