VECTRA
SECURITY THAT THINKS®

ソリューション概要

サイバー攻撃による製造業のビジネスリスクを低減するには

製造業は長年、産業用制御システムを使って生産現場のスピードや効率を向上させてきましたが、こうした生産管理システムの多くは、業務管理システムやエンタープライズシステムとは別に縦割り運用されていました。

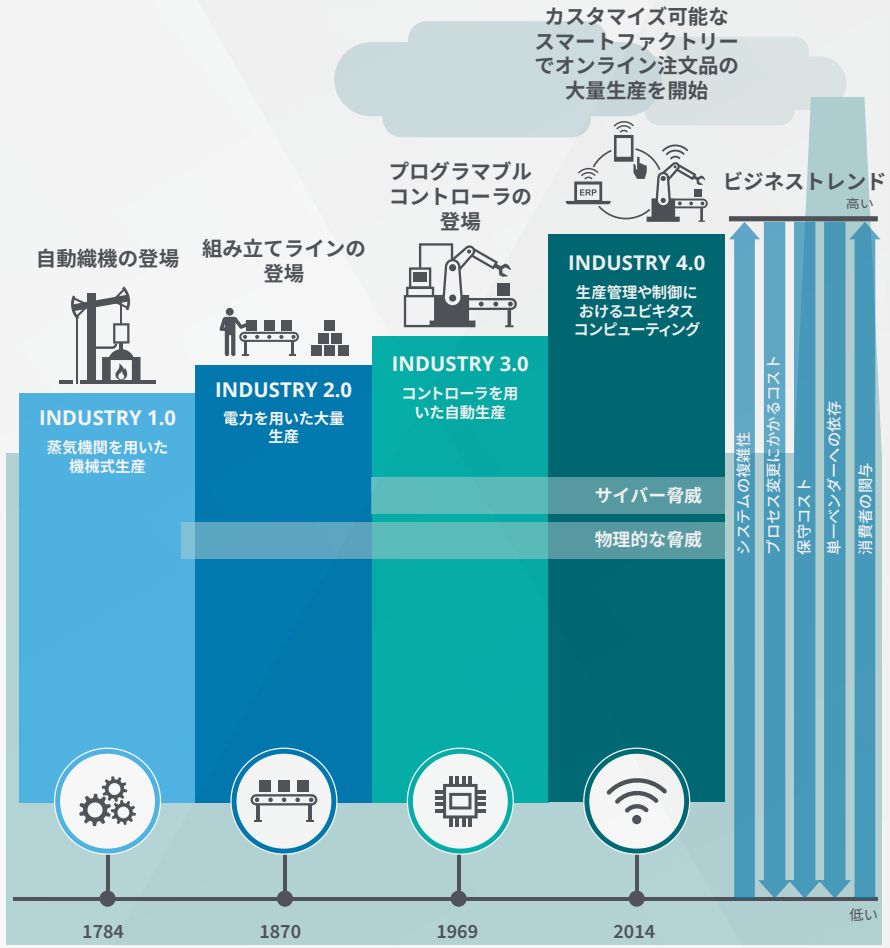
こうした時代はもう終わりです。

Industry 4.0の到来により、製造業は複雑なデジタルシステムやインダストリアルIoT (IIoT) デバイス、クラウドコンピューティング・リソースを統合し、分析能力、自動化、最適化をさらに高めることで、他社との差別化を競っています。その結果、OT (Operational Technology) ネットワークとIT (Information Technology) ネットワークとの融合が進んでいます。

製造業では、多種多様なスマートIIoTデバイスが大規模ネットワークに接続しています。エッジやクラウドにデータをコンスタントに供給するIIoTデバイスやセンサーがひとつの工場に何万個も設置されていることもあります。

製造業ではこのほか、監視カメラ、デジタルサイネージ、ビルオートメーション、環境管理システムなどのエンタープライズ向けIoTデバイスも数多く使われています。IIoTシステムのセンサーや機器と同様、こうしたスマートデバイスの多くは最近開発された技術のため、セキュリティに関する実績が不十分です。

エッジやクラウドにデータをコンスタントに供給するIIoTデバイスやセンサーがひとつの工場に何万個も設置されていることもあります。



出典：Deloitte

Deloitte University Press | dupress.deloitte.com

内在的なサイバーリスク

Industry 4.0の到来によって、スマートファクトリーやデジタル化されたサプライヤーネットワークに新たなオペレーショナルリスクが生まれました。オペレーションの各要素が相互連携し、デジタル変革が急速に進む環境でサイバー攻撃を受けると、かつてないほどの被害につながる恐れがあります。

製造業およびサプライヤーネットワークは、こうしたリスクへの備えが不十分である恐れがあります。さらに、IIoTデバイスやクラウド、ますます高まる相互接続性があいまって、これまで製造業が経験したことのない膨大な攻撃対象領域が生まれます。偵察やマルウェア拡散、情報窃取などを企むサイバー犯罪者にとって、製造業のシステムに侵入することは、これまでよりずっと容易になっているのです。

「先日、米国の電力制御システムが国家ぐるみのサイバー攻撃を受けたという報道がありました。サイバー犯罪者が重要な産業資産や知的財産の存在場所を内密に調べ上げ、米国における生産活動を混乱させようという意図がうかがえます。」

Frost and Sullivan インダストリーディレクター
Vikrant Gandhi氏

製造業の組織がIndustry 4.0時代におけるサイバーリスクに立ち向かうには、何らかのイベントが発生次第、検知して対応可能な可視性および即応体制を整備する必要があります。

今日の製造業におけるセキュリティオペレーションには、ネットワーク全体をリアルタイムかつ自動で分析し、進行中の脅威が実害をもたらす前に検知および対応できる体制が求められます。

製造業を狙うサイバー攻撃者の振る舞い

製造業では、ネットワーク内部での悪質な振る舞いの件数がネットワーク外の攻撃行動より圧倒的に多く、全般的に見ると2対1の割合で「侵入後の横展開（ラテラルムーブ）」の比率が「コマンド&コントロール攻撃」を上回っています。

このことから、製造業のネットワークには安全でないIIoTデバイスが大量に存在し、内部のアクセス制御が不十分なため、いったん侵入されると簡単に、あっという間に攻撃が拡散し得ることがわかります。

製造業のなかには、業務上の理由によって生産ラインのセキュリティアクセス制御を不十分な状態にしている企業もあります。アクセス制御が働くと、リーン生産ラインとデジタルサプライチェーンプロセスに不可欠な生産システムが中断され、他のシステムから隔離される可能性があるためです。

多くの工場では、パーティション分割されていないフラットネットワークにIIoTデバイスを接続し、汎用的演算デバイスやエンタープライズアプリケーションと通信します。こうしたデジタルファクトリーでは、インターネット対応の生産ラインを導入し、遠隔測定データの収集や遠隔管理を行っています。

「インダストリアルIoTデバイスではエージェントベースのソリューションを適用できないため、社内ネットワークを常時監視し、アクセス制御を厳格化して攻撃者の振る舞いをすぐに識別できるよう備えておくことが重要です。」 Brugg Cables社 CIO **Jürg Affolter氏**

これまで製造業は、各社各様にカスタム開発したプロトコルを使っていたため、サイバー犯罪者が攻撃を仕掛けにくい構造でした。しかし、プロトコルを標準プロトコルに移行することで、製造業のネットワークインフラに侵入しやすい状況が生まれています。

Brugg Cable社のCIOであるJürg Affolter氏は「インダストリアルIoTデバイスの普及により、製造業における攻撃対象領域が飛躍的に拡大します。これらのデバイスではエージェントベースのソリューションを適用できないため、社内ネットワークを常時監視し、アクセス制御を厳格化して攻撃者の振る舞いをすぐに識別できるよう備えておくことが重要です」と話しています。

コマンド&コントロール

製造業のネットワークへの悪質なコマンド&コントロール攻撃に最もよく使われる振る舞いが、リモートアクセスツールによる外部からの侵入です。外部からのリモートアクセスは、ネットワーク内部のホストデバイスが外部サーバーに接続する際に発生します。

その場合、攻撃活動は、通常のクライアントからサーバーのアウトバウンドトラフィックとは逆の振る舞いになります。外部サーバーの指示をクライアント側が受け、外部の人間が相互通信をコントロールします。

外部からのリモートアクセスは製造業にとって日常的なオペレーションですが、リスクも発生します。こうしたリモートアクセスが、産業用制御システムの妨害を企むサイバー攻撃者に悪用される恐れがあるためです。

ネットワーク内部の偵察

IIoTデバイスは、攻撃展開の踏み台として使われることがあります。IIoTデバイス上に攻撃の足場を固められると、ネットワークセキュリティシステムでバックドア経由の侵害を特定することが困難になります。

> IIoTデバイスは、攻撃展開の踏み台として使われることがあります。

その結果、IIoTデバイス全体が大規模で侵入しやすい攻撃対象領域となり、重要資産の窃取や、インフラ破壊を狙うサイバー犯罪者による内部偵察を許してしまいます。

製造業でよく見られる内部偵察の振る舞いは、ネットワーク内部のダークネットスキャンやSMBアカウントのスキャンなどです。ネットワーク内部のホストデバイスがネットワークに存在しない内部IPアドレスを検索する際に、ダークネットスキャンが実行されます。

ホストデバイスがSMBプロトコル経由で複数のアカウントを立て続けに使用する際には、SMBアカウントスキャンが実行されます。これらのアカウントが、ファイル共有やRPCをはじめとするラテラルムーブの振る舞いに使用される可能性があります。

製造業のネットワークは、スマートデバイスやマシンと通信する多数のゲートウェイで構成されています。これらのゲートウェイはピアツーピア(P2P)通信を簡素化するためにメッシュ型トポロジーで相互接続しています。サイバー攻撃者はP2P対応デバイスと同じ自己検出機能を使って標的ネットワークの詳細構造を把握したうえで、窃取または破壊の対象となる重要資産の保管場所を探します。

ラテラルムーブ

接続されたシステムとデバイスがネットワークを介して相互通信する際、ラテラルムーブが発生します。製造業では認証関連のラテラルムーブが多く見られ、SMBアカウントの総当たり攻撃も頻繁に発生しています。

> IIoTシステムは、攻撃者がネットワーク全体を横移動しやすい環境を生み出してしまいます。

SMBアカウントの総当たり攻撃は、内部ホストがSMBプロトコルを利用して、同一ユーザーアカウントにログインを複数回試行する際に発生しますが、通常は失敗に終わります。その結果、内部ホストデバイスが同じようなペイロードを数種類の内部ターゲットシステムに送信しているという痕跡（大量の自動レプリケーション）が発見されることもあります。

IIoTシステムは、攻撃者がネットワーク全体を横移動しやすい環境を生み出してしまいます。攻撃者は標的ネットワークの基幹業務システムや周辺サブシステムの間を自由に移動し、遂行可能な任務を完了するための経路を見つけ出そうと試みます。

正規ユーザーによる振る舞いと、ネットワーク内部で拡散する攻撃行動の違いを把握できるよう、ネットワーク上の接続システムすべてを常に可視化しておくことが不可欠です。

データの持ち出し

製造業におけるデータ持ち出しで最もよく見られる振る舞いのひとつが、データ・スマグリング(smuggling)です。この振る舞いでは、外部の攻撃者に乗っ取られた内部ホストデバイスがひとつまたは複数の社内サーバーから大量のデータを取得し、大容量のデータペイロードを外部システムに送信します。

また、複数のセンサーがエッジゲートウェイで収集したデータをクラウドに送信し、監視・分析を行うIIoTネットワークのアーキテクチャでは、こうした振る舞いが発生しやすくなります。

このようなIIoTベースのアーキテクチャは、製造業では一般的であり、通常は攻撃行為には該当しません。

製造業におけるデータ持ち出しでよく見られる振る舞いはデータ・スマグリング(smuggling)です。

データの持ち出しは通常、攻撃のライフサイクルにおけるその他の脅威と関連した振る舞いのため、何らかの攻撃が「進行中」であることが示唆されます。社内システムからデータを送信する際は、相手先に間違いがないこと、かつ承認を受けた外部システムであることを確認し、知的財産、事業計画、営業機密などの窃取を企む攻撃者の手にデータが渡らないように徹底することが不可欠です。

AIを駆使したサイバー攻撃検知および脅威ハンティング

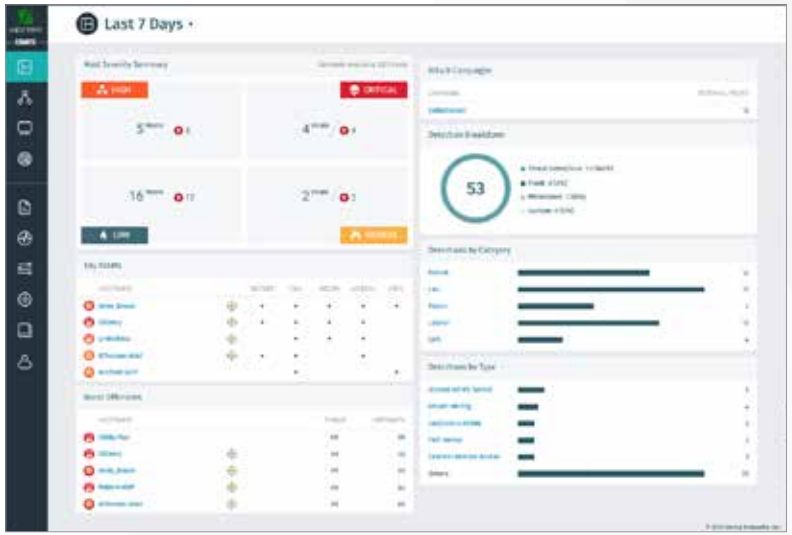
悪質な攻撃にさらされる今日のデータ環境では、包括的で全社横断的な脅威検知および対応策が必須です。新たな産業革命をもたらすスマートマニュファクチャリングの進展に伴い、攻撃リスクはかつてないほどに高まっています。

Vectra AI社は、人工知能を駆使し、高度なサイバー攻撃のリアルタイム検知および対応サービスを提供する世界的リーダーです。

AIを活用した当社製品の代名詞であるCognito®プラットフォーム（脅威検知・対応製品）は、隠れたサイバー攻撃者を自動検知し、脅威ハンターによるインシデントの徹底調査を支援します。Cognitoプラットフォームの重要な構成要素であるCognito Detect™およびCognito Recall™は、いずれもAIを活用したパワフルなアプリケーションです。

Cognitoプラットフォームは、脅威を常時監視し、ネットワーク内部で隠れて拡散し続ける未知のサイバー攻撃を先回りして自動的にあぶり出します。クラウドやデータセンターのワークロードから、ユーザー、IIoTデバイスに至るまで、あらゆるネットワークトラフィックをCognitoプラットフォームが絶えず監視し、分析します。

Cognitoが検知した脅威は、攻撃を受けたホストデバイスに自動で関連付けされるため、セキュリティオペレーション部門は「最もリスクの高い脅威」を直感的な画面で



検知した攻撃に対して優先順位やスコアがその場で付与され、侵害されたホストデバイスとの相関関係が表示されます。

確認できます。また、インシデントの徹底調査の材料となるフォレンジックエビデンスも提供します。

Cognitoが収集・使用するデータは、サイバー攻撃発生時に信頼できる唯一の情報源「ネットワークトラフィック」です。企業のデータセンターからパブリッククラウド、IT/OT一体型環境まで、あらゆるネットワークを行き来するトラフィックのみが、現状を忠実に再現し、真実を明らかにする唯一の情報源となります。境界型セキュリティ対策では、検知の網をすり抜けて内部に潜む攻撃を確認できません。

Cognitoは、機械学習、データサイエンス、振る舞いベースのトラフィック分析を組み合わせ、攻撃者によるコマンド&コントロール、内部偵察、ラテラルムーブ、データ持ち出しなどの振る舞いをあぶり出します。さらに、暗号トラフィック上の脅威を復号せずに検知することもできます。

信頼できるユーザーの認証情報が攻撃者によって侵害された際も、Cognitoが検知します。内部のKerberos認証インフラを追跡管理し、正常なユーザーの振る舞いを覚え込むことで、管理者用認証情報の不正使用や、IPMIなどの管理プロトコルの悪用を検知します。

Cognitoは、セキュリティ・エコシステム全体をスムーズに連携するうえで大変重要な役割を担っており、業界をリードする数々の他社製品（ファイアウォール、エンドポイント検知および対応製品、SIEM、仮想プラットフォーム、トラフィック最適化ツール、オーケストレーションソリューションなど）と統合可能です。

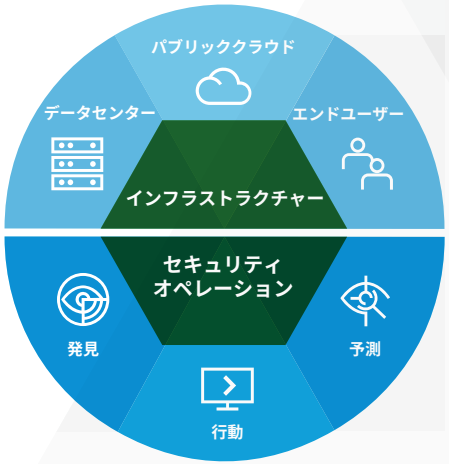
「Vectra製品が攻撃者を自動検知してくれるため、
我々は最も重大な脅威にいち早く対応できます。」

Vetropack Group
ITインフラ・運用部門責任者
Markus Müller-Fehrenbach氏

人間 + AI = Security that thinks®（自ら思考するセキュリティソリューション）

製造業は今後とも、サイバー攻撃の格好の標的となることが予想されます。しかしご安心ください。製造業のセキュリティ部門でCognitoプラットフォームをご活用いただくことで、これまでにないスピード、正確性、効率性をもって対応し、被害が及ぶ前に脅威を検知・軽減できます。

Cognitoプラットフォームは、サイバー攻撃をリアルタイムで自動検知し、AIを活用した脅威ハンティングサービスを提供します。セキュリティご担当者はこれらの情報にコンテキストを補足したり、クリティカルシンキングの手法を適用することができます。人間とAIの力を組み合わせて脅威を迅速に特定し、阻止することで、データ窃取やスパイ活動、業務妨害から製造業を守ることができるのです。



Cognitoプラットフォームは、人工知能を駆使した機能でセキュリティオペレーション部門の業務を補完し、クラウドやデータセンターのワークロードからユーザー、IIoTデバイスまで様々な場所で発生する脅威を可視化します。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp