The bridge to possible

IT と OT のサイバーセキュリティ：統合された組織と分断された組織

産業界の環境は変化しています。Industry 4.0 や Internet of Things（IoT）などのテクノロジーの進化により、新たな運用テクノロジー（OT）が登場しています。これらの最新技術は、産業用ネットワーク内のサイバーセキュリティ対策をはるかに上回るペースで導入されています。設計上安全ではない老朽化した環境をそのペースに合わせて保護することは、多くの組織にとって悩みの種であると言えます。OT と IT が密接に関連するようになったことで、セキュリティを強化するには両分野の取り組みを統合する必要が生じています。

IoT デバイスは、OT ネットワークで大きな役割を担い始めています。IP カメラが重要なシステムをモニターし、製造現場のスマートセンサーが、貴重なデータをクラウドに直接送信しているからです。このような発展により品質が向上し、プロセスがこれまでになく迅速に実行されるようになりました。しかし、これらの発展にはリスクが伴うだけでなく、産業環境に脆弱性が残る危険性さえあります。

産業用ネットワークと重要な産業用制御システムを保護する方法に関して多くの仮定が立てられていますが、それらはもはや成り立っていません。「システムを隠蔽することによるセキュリティ」、エアギャップ（物理的にネットワークを切り離すことによるセキュリティ）、Demilitarized Zone（DMZ; 緩衝地帯）を確立することによるセキュリティなどの従来の対策では、もはや産業環境を保護しきれないのです。産業用ネットワークを分離しても常に効果があるとは限りません。また、ネットワークを分離すればデータにアクセスできなくなり、再設定やパッチの適用も難しくなります。実際、いわゆるエアギャップシステムの多くには、大量のバックドアが存在しています。その好例は、システムやデバイスを更新する目的で、OT 環境に独自のリモートアクセス機能をセットアップしているベンダーやサードパーティの技術者がいる点です。

産業環境に対するサイバー攻撃の頻度と複雑さが増す中、企業の取締役や政府の規制当局は、このようなリスクを管理し、ビジネスに不可欠な IoT/OT ネットワークを適切に保護することを組織に求めています。その要求に応えるには、IT と OT が対等な立場でコラボレーションするアプローチが必要です。

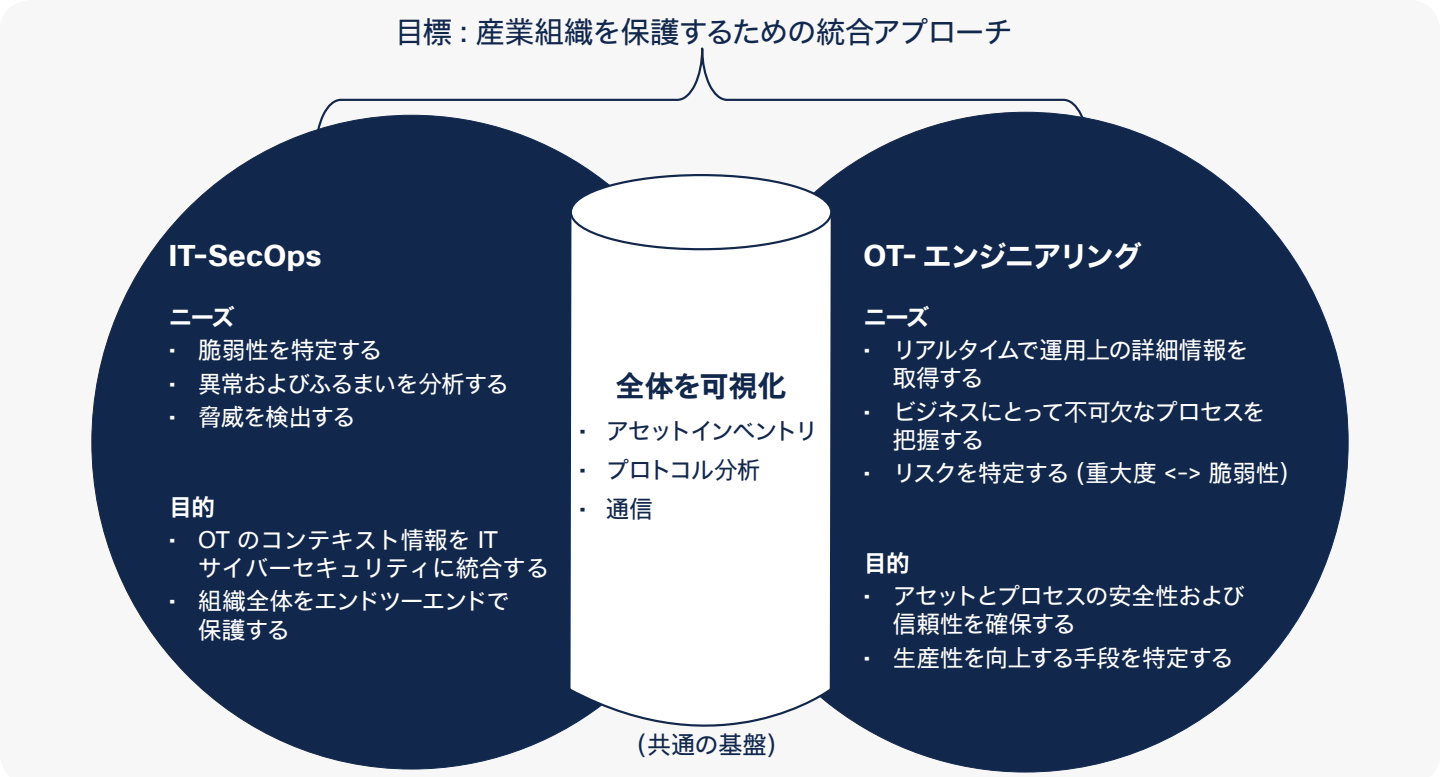
多くの組織では、最高情報セキュリティ責任者（CISO）と IT チームが、サイバーセキュリティに対して全体的な責任を負っています。CISO と IT チームが、企業を保護するために必要なツール、専門知識、方法論を擁し、また多くの場合は予算も管理しています。一方、IT および SecOps の担当者が、運用テクノロジーやプロセス制御テクノロジーに関して必要な専門知識や知見を持っていることはほとんどありません。この知識ギャップにより、IT 担当者と SecOps 担当者は、IT を保護するためのアプローチを OT 環境にも適用できると考えてしまいがちです。

The bridge to possible

産業組織を保護するには、IT チームと OT エンジニアが連携する必要があります。そして、保護しなければならないアセットを共同で把握し、生産活動を中断することなくそのアセットを保護する方法を調査して深く理解しなければなりません。このように IT と OT が協力しあうには、双方に何らかのメリットが必要です。

すべてのニーズに対応

図 1. IT と OT を統合してリスクを特定し、セキュリティを確保する



IT 担当者と OT 担当者の運用手順と役割は異なり、それぞれの見方は大きく異なります。ただし、企業を保護するという点についての目標は同じです。その目標を達成するためには、共通の基盤を確立する必要があります。

OT エンジニアは、IoT/OT ネットワークを構築し、そのネットワークに接続するデバイスを維持する役割を担っています。これらのシステムの動作は一貫している必要があります。また、多くの場合、その動作環境は過酷です。システムとアセットの完全性は最優先事項で、障害が発生したりダウンしたりするとコストがかかり、大きな問題になる可能性があります。

OT の担当者は、安全性、信頼性、生産性に重点を置いています。その役割は、人、生命、環境、運用、生産を保護することです。

一方、サイバーセキュリティ担当者は、情報の秘密と IT システムの完全性 / 可用性を維持することに重点を置いています。

ただし、両者の目標には共通する部分があります。どちらも、組織の保護、リスクの最小化、稼働時間の最大化および、組織が安全に収益を創出し続けられるようにすることを目標としています。

OT と IT が明らかに別のものであるという考え方は時代遅れです。OT と IT の関係がますます強まっているということを認識していないと、産業組織を正しく運用できない可能性があります。OT 部門と IT 部門がお互いに信頼しあって理解し、協力できていないと、組織のセキュリティ態勢に大きな悪影響が及びます。

通常、IT サイバーセキュリティに関する取り組みは、CISO によって推進されます。CISO は、情報、アセット、テクノロジーを適切に保護するために、企業のビジョン、戦略、プログラムを策定して維持する役割を担っています。

産業界の多くの企業では、最高リスク管理責任者（CRO）も任命されています。CRO は、組織の収益性と生産性を低下させるようなビジネス上のリスクを軽減する役割を担います。特に、重要なインフラストラクチャを運用している企業は、リスクの概念に非常に精通しています。

ただし、役職にかかわらず、産業環境の保護を担う責任者は、組織の IT と OT の両方を同じように重視する必要があります。OT チームは、生産を継続し、ダウンタイムを短縮するために、アセットとプロセスを可視化する必要があります。一方セキュリティチームは、主要なインシデントだけに重点をおいてモニターすればよく、ネットワーク内のすべての変化をモニターする必要はありません。

両者が同じものを見えているか

ほとんどの産業組織では、IT サイバーセキュリティ部門と OT 部門が分断されています。全体を可視化できることはほとんどなく、お互いがどのように運用されているかについてはあまり理解されていません。

OT システムのライフサイクル（15 ～ 30 年以上）は、IT システムのライフサイクル（3 ～ 5 年）よりもはるかに長くなっています。デバイスとコンポーネントはビジネスに不可欠なプロセスの一部であるため、停止することはほとんどなく、まったくないことも珍しくありません。OT 環境では、「定例のパッチ適用日」のようなものはありません。IT 部門が長年にわたって IT 環境で安全に使用してきたプロセスを、OT 環境にそのまま適用することはできません。

IT セキュリティソリューションが OT 環境に導入される場合、OT 環境が理解されないまま導入されることがよくあります。IT 担当者は、OT 環境とその仕組みについて理解していないことが多く、基本的な情報も把握できていません。また、サイバーセキュリティに関する意思決定は、OT エンジニアの意見が考慮されずに行われることがよくあります。その結果、適切に導入されずにダウンタイムが発生し、OT エンジニアは、新たなシステムを導入することに抵抗するようになります。

セキュリティ対策を確実に実施するためには、IT チームと OT チームが、サイバーセキュリティ プロセスの各フェーズで協調して作業する必要があります。プロセスの初期段階からコラボレーションすることは、成功するための重要な要素です。

共通の基盤を構築して連携する

OT チームとサイバーセキュリティチームの見方が異なるのは当然で、連携するためには共通の基盤を構築することが重要です。IEC 62443、ISO 27001、NIST、CPNI、ENISA などの両者に共通の標準規格やサイバーセキュリティ フレームワークに基づいて連携することで、それぞれの組織の役割と責務に対する理解を深めることができます。

たとえば、IT と OT のアプローチの主な違いのいくつかは、米国国立標準技術研究所（NIST）の SP 800-82 標準で示されています。IT システムでは再起動することは認められていますが、OT システムでは認められていません。同様に、IT システムの多くは停止することが許容されていますが、OT システムの変更は、スケジュールされたメンテナンス期間にのみ行われ、システムの停止は、数週間または数ヵ月前に計画してスケジュールを策定しておく必要があります。たとえば、OT 環境にパッチを適用することは、IT 環境とは大きく異なり、非常に困難なプロセスです。脆弱性を特定してからパッチを適用できるようになるまでの期間は、サプライチェーンに影響が及ぶため、多くの場合かなり長くなります。また、老朽化したテクノロジーの場合は、徹底的にテストしてから慎重に対応する必要があるため、さらに長くなります。

OT システムの要件を考慮したアプローチを構築することは、信頼して受け入れてもらうために最も重要です。

The bridge to possible

ビジョンを共有することの価値

NIST は、重要なインフラストラクチャに対するサイバーリスクを軽減するために、サイバーセキュリティ フレームワーク（重要インフラのサイバーセキュリティを強化するためのフレームワーク）を開発しました。産業界の組織が OT セキュリティプロジェクトを円滑に開始できるように、標準、ガイドライン、ベストプラクティスが提供されています。

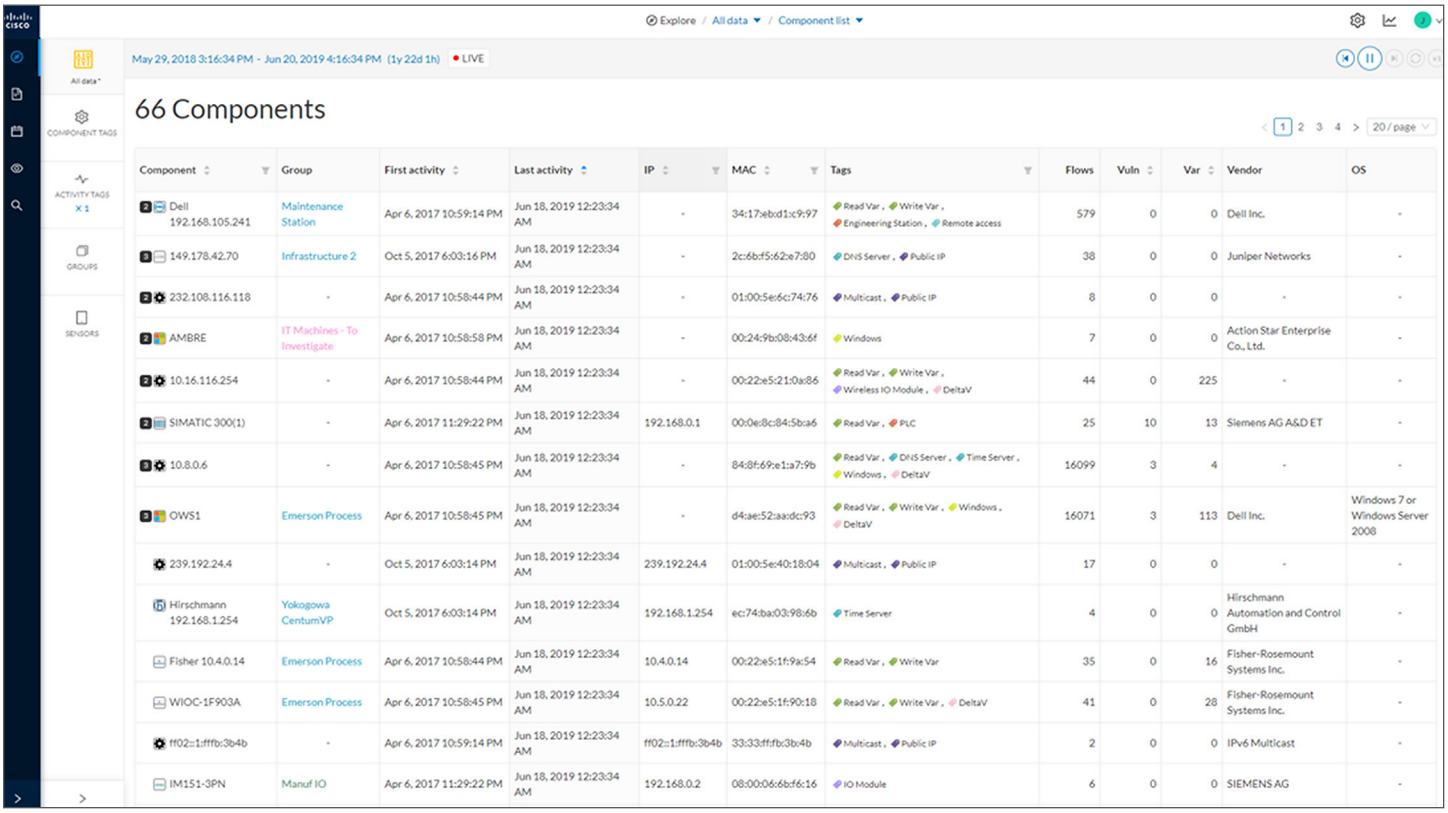
ステップ 1：特定

NIST サイバーセキュリティ フレームワークの最初の機能は、「特定」機能です。特定機能には、物理的なアセットだけでなく、組織を構成するデータ、要員、デバイス、システム、機能、設備を特定する機能も含まれています。包括的なリスク管理戦略を策定するには、重要な機能をサポートするリソースと、関連するサイバーセキュリティリスクの両方をすべて理解する必要があります。一言で言うと、一番重要なのはコンテキストです。

産業環境を保護するには、デバイスが環境に設置されてから取り外されるまでのすべての段階で、環境内のすべてのデバイスを継続的に可視化する必要があります。可視化することで、組織は、脆弱性、ベンダー向けのリモートアクセス機能、廃棄されたアセットをトラッキングできます。

検出プロセスでは、デバイス、ファームウェア、ウイルス対策ソフトウェアなどのシステム要素の製造元とモデルの情報が特定され、アセットの脆弱性を評価するためのアセットインベントリが自動的に構築されます。またこのステップには、ネットワークをリアルタイムで可視化するためのネットワーク検出プロセスも含まれます。

図 2. Cisco Cyber Vision の詳細なアセットインベントリ画面

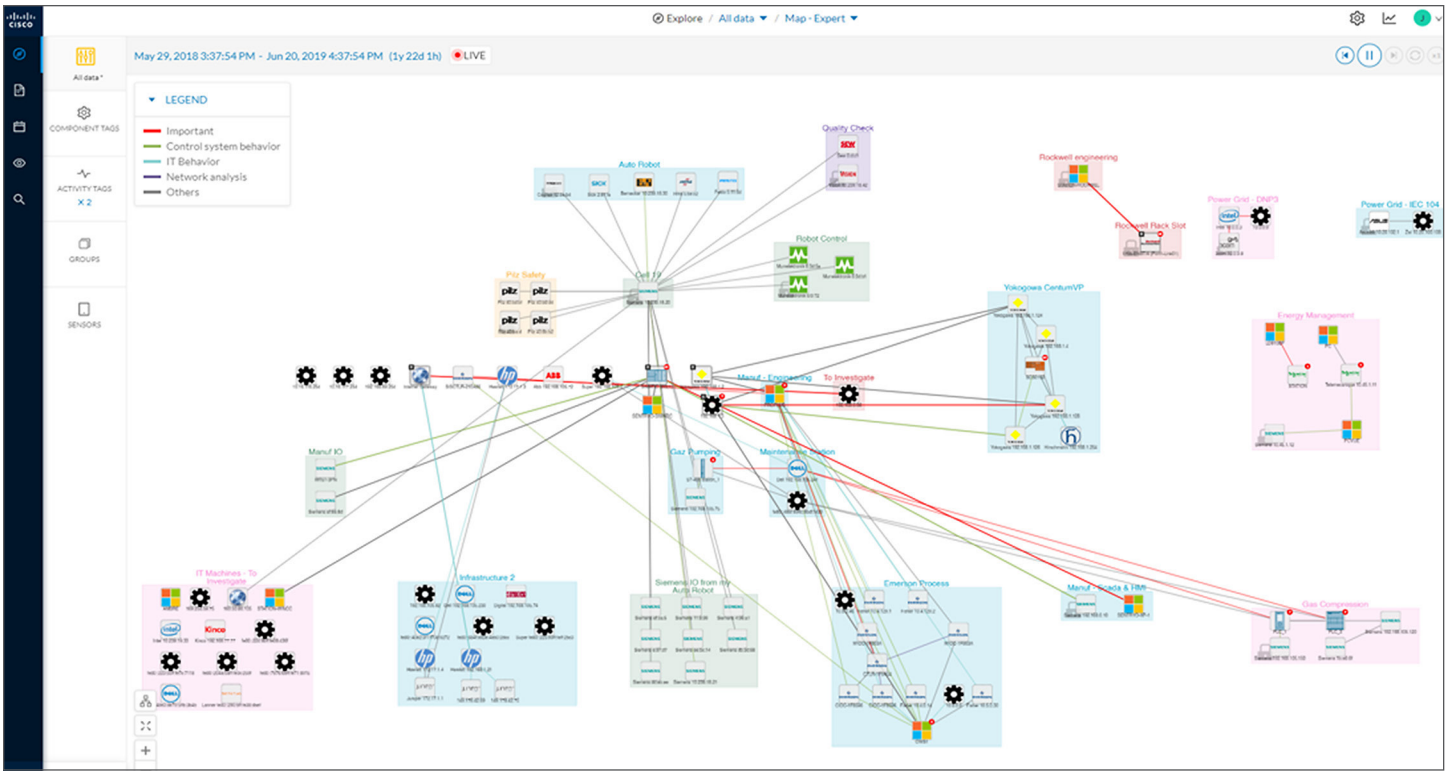


このフェーズの主要な成果物は、ビジネスプロセスのリスク分析結果です。IT/SecOps チームと OT チームが連携することで、主なプロセスを表すグループにアセットを分類し、それらのグループが相互に通信する方法および、組織における重要度を定義できます。また、重要度に従って各グループのイベントアラートに優先順位を付けることができます。

ここでの OT チームの役割は重要です。OT チームは、ビジネス機能の面から重要度を特定する役割を担います。OT チームは、OT ネットワークとアセットのリアルタイムビューを利用することで、アセットに対する生産面での影響を定義し、各アセットの重要度レベルに基づいてイベントに優先順位を設定できます。この手順は、効果的な検出戦略を策定し、セキュリティ オペレーション センター（SOC）が大量のイベントに疲弊してしまわないようにするために必要です。

IT/SecOps チームと OT チームは、コンテキストに基づいて、産業環境を包括的に把握する必要があります。包括的で詳細なアセットインベントリ、デバイス間の通信状況の把握機能、産業プロセスに関するリアルタイムの分析機能は、変化する環境において特に重要です。

図 3. アセット、インタラクション、ビジネスコンテキスト（プロセス）を確認できる Cisco Cyber Vision ネットワークマップ



OT エンジニアは、このマップを確認することで、さまざまな条件下で OT ネットワークがどのように動作しているかを明確に把握し、安全性と生産の継続に関する適切な計画を策定できます。また、IT サイバーセキュリティチームと連携して、重要なビジネスプロセスと関連デバイスを文書化できます。これらの活動は、IT/SecOps チームが OT チームに受け入れられやすい手順を策定し、ビジネスプロセスをより安全に保護するための構想を練るのにも役立ちます。IT/SecOps のスペシャリストと SOC アナリストが OT のコンテキストを取得して理解し、知識を得ることは、組織全体のサイバーセキュリティに関する目標を達成するために不可欠です。

ステップ 2 : 保護

ネットワークに接続されたデバイス、プロセス、設備を一元的に管理して明確に確認できるようにすれば、IT/SecOps チームと OT チームが連携して、IoT/OT 環境を保護するための共同戦略を策定できます。つまり、産業環境が無駄なく効率的に稼働し続けるための適切な保護対策を構築して導入できるということです。

NIST サイバーセキュリティ フレームワークの保護機能は、潜在的なサイバーセキュリティ イベントの影響を限定または阻止する機能をサポートするものです。そのためには、ISA99/IEC 62443 モデルで説明されているように、産業用ネットワーク内のさまざまな要素を、コンジットで接続されたゾーンに分離するネットワークアーキテクチャを設計する必要があります。

通常このようなネットワークアーキテクチャにはネットワーク セグメンテーション機能が含まれます。その目的は、ビジネスに不可欠なプロセスで利用するデバイスを保護し、セキュリティ脅威やサイバー攻撃者がネットワークを介して自由に水平移動できないようにすることです。組織は、ネットワークをセグメント化することで脅威を分離し、ネットワーク内の最も重要な部分で脅威を検出することに注力できます。

Cisco 3000 シリーズ産業用セキュリティアプライアンス (ISA 3000) などの産業界に特化したソリューションを利用してセグメント化することで、IT 部門と OT 部門が連携し、製造セル、産業ゾーン、変電所などを分離するためのローカル フィルタリング ルールを作成して、承認されたデバイスや接続のみにアクセスを許可できるようになります。その結果、悪意のあるアクティビティや不要なアクティビティからネットワークが保護されます。さらに、「OT 対応」ファイアウォールが、脆弱性があってもパッチを適用できないデバイスを保護するレイヤとなります。

ネットワーク セグメンテーションは、Cisco Identity Services Engine (ISE) などのネットワーク アクセス コントローラ (NAC) を利用して実装することもできます。このソリューションには、次世代ファイアウォールのようなフィルタリング機能や脅威検出機能はありませんが、組織は、アイデンティティとプロファイルに基づいてアセットが相互に通信するのを許可 / 拒否することで、セキュリティポリシーを簡単に実装できます。ネットワーク機器は、このようなポリシーを適用するように自動的に設定されます。

これらの NAC プラットフォームは IT チームによって管理されますが、OT のサポートなしでは産業用ネットワークをセグメント化することはできません。セキュリティポリシーを設定するためには、これらの各産業用アセットのプロファイルをプラットフォームに追加する必要があります。Cisco Cyber Vision などの製品を利用してアセット情報をツールに継続的に送信すれば、プロファイルを自動的に追加できます。

さらに重要なことは、OT エンジニアリングチームは、適用するポリシーを定義する必要があるということです。OT エンジニアリングチームは、どの通信を禁止すべきかや、生産が中断しないようにするためにはどの通信を許可する必要があるかを把握しています。IT チームと OT チームが連携し、アセットグループ (ゾーン) と通信ポリシー (コンジット) を手動で定義することで、このような IT と OT のコラボレーションを実現できます。また、OT チームが Cisco Cyber Vision などのツールを使用してロジックを設定し、Cisco ISE と自動的に共有することで、IT チームは、適切なセキュリティポリシーを設定するために必要な情報も得られます。

ステップ 3 : 検出

NIST サイバーセキュリティ フレームワークの検出機能には、サイバーセキュリティ イベントの発生を特定するための適切なアクティビティを開発して実装する機能が含まれています。

運用環境に導入される IT のコンポーネントが増えるにつれ、産業用ネットワークで IT に対する脅威を検出することがますます重要になっています。脅威を検出するには、エンドポイント保護テクノロジーと侵入検知 / 保護テクノロジーを組み合わせる必要があります。

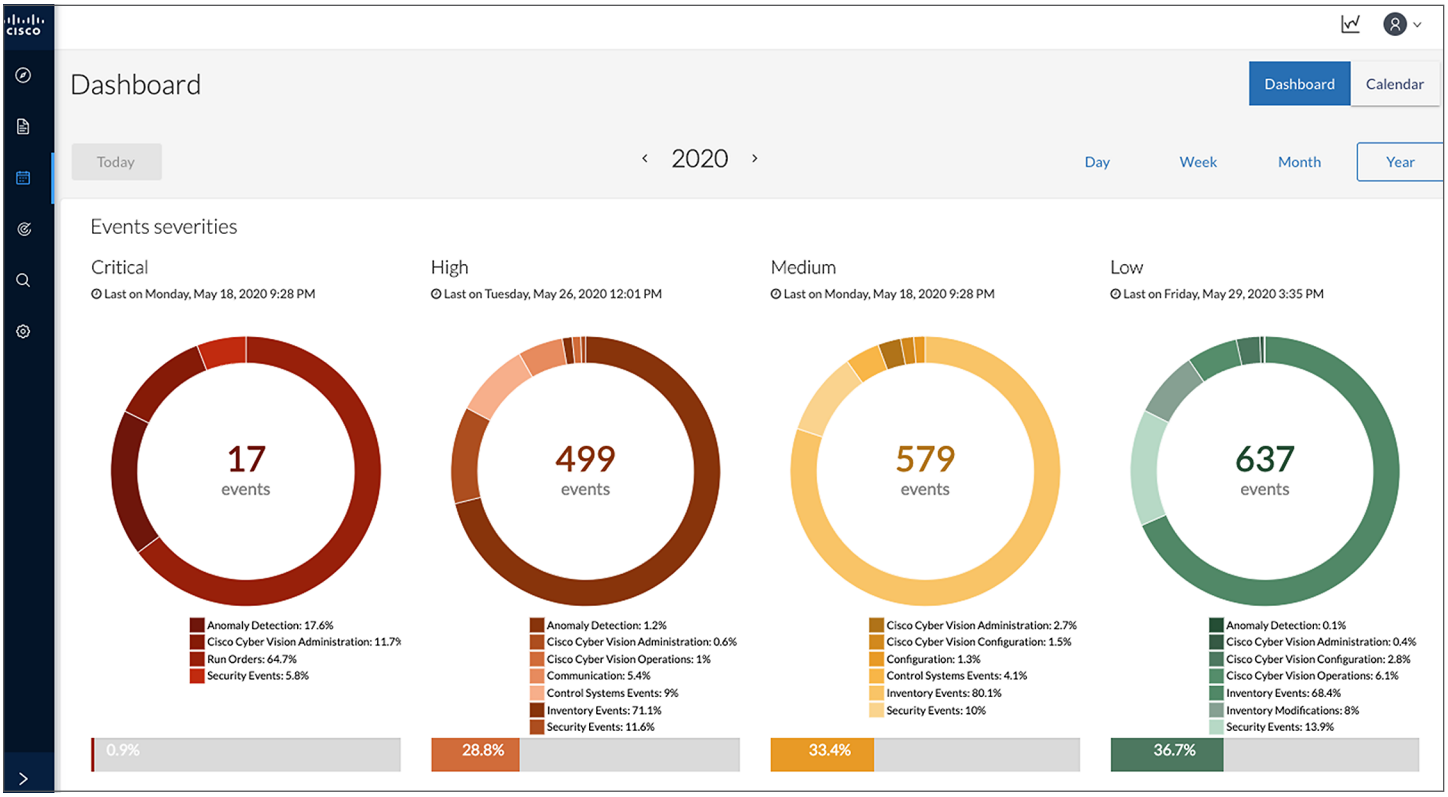
たとえば、ネットワークをセグメント化するために導入されるセキュリティアプライアンスには、マルウェアや悪意のあるトラフィックを検出できる機能が含まれている必要があります。しかし、これらの次世代ファイアウォールも重要ですが、ファイアウォールがさまざまな既知の脅威や新たな脅威を効率的に検出できるように、組織には Cisco Talos や Cisco AMP for Networks などの脅威インテリジェンスフィードも必要です。

また、継続的にセキュリティをモニターする機能も実装し、データの完全性を確認する必要があります。データの完全性は、一般的に IT セキュリティに関するものと考えられていますが、産業用ネットワークトラフィックを解析し、トラフィック内のコマンドの完全性と正当性を判断することでプロセスの異常をチェックする場合には、OT セキュリティにも当てはまります。組織は、産業環境で使用されるプロトコルを理解し、OT のプロセス、環境、アセット、プロトコルの正しい利用方法を把握しているソリューションを必要としています。

IT 担当者と OT 担当者は連携して、どのような状態を異常と判断するかを定義する必要があります。その活動には、通常の産業プロセスの状態を定義する、異常な状態による影響を把握して重大度レベルを設定する、および、IT チームと OT チーム間の効果的なコミュニケーションを実現する（たとえば、OT のメンテナンス中に誤ったアラームを発生させて SecOps チームを混乱させないようにするなど）ことが含まれます。

組織の各部門は、日々の活動の中で OT セキュリティイベントを評価して調査 / 対応するために、さまざまな種類のデータや分析情報を必要としています。OT チームは、プロセスの変更やデバイスに対する変更をモニターします。IT/SecOps チームは、脆弱性と IDS イベントをモニターします。そして、SOC マネージャは、調査プロセスとポリシー設定をシンプルにするために、詳細なアセット情報を必要とします。

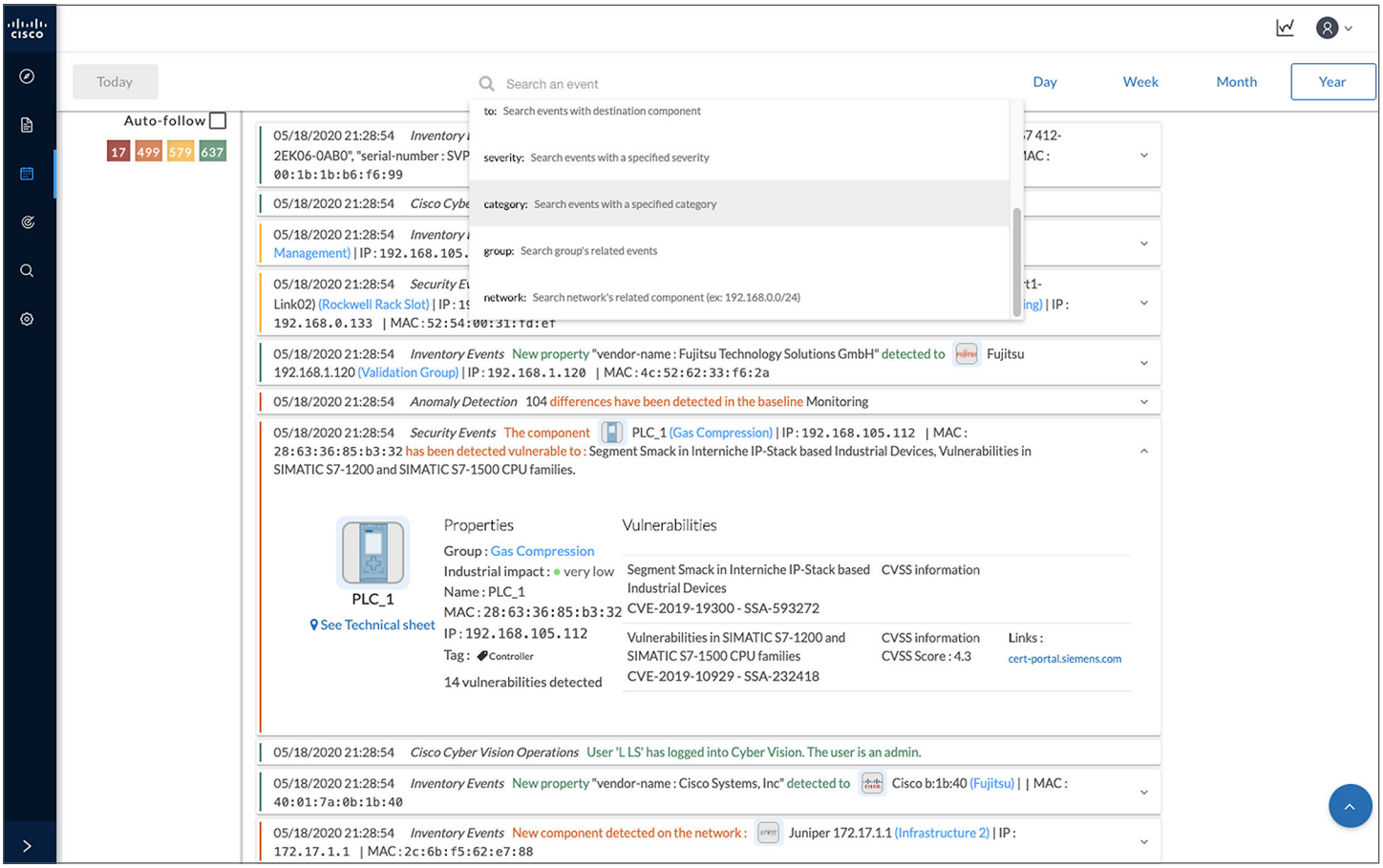
図 4. Cisco Cyber Vision のイベントダッシュボードを利用することで、OT と IT の両方が産業用ネットワークのすべてのイベントをトラッキングできる



IT/OT SOC アナリストは、企業の IT ネットワークと IoT/OT プロセスネットワークの両方を対象とした、サイバーキルチェーンの全体像を把握する必要があります。OT のコンテキストと、IoT/OT ツールを既存の IT/SecOps ツールおよび SOC ツールと緊密に統合する機能を利用することで、これらのチームは、組織全体のサイバーリスクを最小限に抑えるという目標を達成できます。さらに、業種によっては、コンプライアンスや規制に対応するためにも同様の詳細情報が必要になることがよくあります。

The bridge to possible

図 5. Cisco Cyber Vision を利用して、OT/IT SOC アナリストが OT コンテキストを理解して解釈できるようにイベントに追加



共通のビジョンをセキュリティアーキテクチャに組み込む

IT NetOps チームは、一般的な OT ネットワークの規模、複雑さ、分散範囲を考慮し、ネットワークを中断させることなく、適切なコストで拡張できるソリューションのみを評価します。

第 1 世代の OT 専用サイバーセキュリティ プラットフォームでは、スタンドアロンのハードウェアベースのセンサーが必要でしたが、次世代の IoT/OT サイバーセキュリティ プラットフォームでは、ネットワーク機器にセンサー機能（特にディープ パケット インスペクション（DPI）機能）を組み込んだ、より実用的な方法が採用されています。産業用ネットワークに DPI 機能を組み込むことで、物理デバイスを利用するよりもはるかに広範囲で対応することが可能なため、大幅に少ない総所有コスト（TCO）で多くの情報を取得できるようになります。また、ハードウェアを削減できることによるメリットもあります。

Switched Port Analyzer(SPAN; スイッチドポートアナライザ) ポートに接続された物理センサーアプライアンスでは、産業用ネットワーク機器からデータを収集するために、ネットワークリソースを追加する必要があります。重要なのは、IT NetOps チームがソリューションを簡単に導入して維持できるように、スペースとネットワークへの影響を最小限に抑え、OT サイバープロジェクトが成功するようにサポートすることです。コスト効率の高い方法で（地理的にも、プロセスネットワークの範囲においても）拡張できるソリューションを選択しなければ、IT NetOps チームが反発し、導入が制限されたり、最悪の場合はプロジェクトが停止したりする可能性もあります。

データの可視性は、さまざまなチームから受け入れてもらうために重要です。各チームの役割にとって有意義なデータを使いやすい方法で提供できるソリューションを利用すれば、チームが状況に関して共通の認識を持ち、すべての関係者に課題解決に参加してもらうことができます。

OT エンジニアリングチームは、生産活動の完全性、継続性、安全性を確保するために、ネットワークの重要な部分にすばやく焦点を絞る、マシンをトラッキングしてゾーンにグループ化する、変数やプロセスの異常を確認するといった対応をできる必要があります。OT エンジニアは、特定のサイトまたは施設を担当する場合もあれば、複数のサイトや地域にまたがる特定のプロセスまたは一連のデバイスを担当する場合もあります。

どのようなアプローチを採用するかは組織によって異なりますが、重要なのは、OT エンジニアに、その役割とタスクに応じた情報を提供することです。OT エンジニアは、テクノロジーを運用する際に利用できる、シンプルで柔軟ながら強力なインターフェイスを必要としています。このようなインターフェイスがあれば、イベントが発生した際に、OT コンテキストを IT/SecOps チームと共有しやすくなります。

IT/SecOps チームおよび SOC チームは、既存の IT セキュリティツールや手順を利用して調査や修復ができ、すべての OT サイトおよび IT サイトを一元管理できる機能を必要としています。そのためには、ソリューションを統合して相互に運用できることが不可欠です（ネイティブの機能または API を利用）。最初のステップは、OT アラートとイベントをセキュリティ情報イベント管理（SIEM）ツールに統合することですが、第 1 世代の OT セキュリティ プラットフォームでは、共有するイベントを選択できません。また、ふるまい分析エンジンをさまざまな生産段階に合わせて調整することもできず、多くの誤検出が発生します。

次世代の OT セキュリティ プラットフォームでは、セキュリティアナリストが SIEM ツールで確認したいイベントを選択でき、OT エンジニアリングチームがさまざまなベースラインを簡単に作成して、モニターする産業プロセスの条件（生産活動の時刻、期間、状態など）に応じてふるまい分析機能を調整できるため、大量のイベントの確認に疲弊してしまうことがなくなります。

IT 部門は、サイバーキルチェーンに従って、組織全体の脅威調査に責任を負います。多くの場合 IT セキュリティチームは、OT ネットワークやデバイスに関してほとんど情報を持っていません。持っていたとしても、MAC アドレスと IP アドレスぐらいです。デバイス名、タイプ / 特性、ビジネス上の重要性などの OT アセット情報を既存のセキュリティツールと共有することで、IT ドメインと OT ドメインの両方で効果的に調査できるようになります。

一方、SOC では、データを相互に参照して自動的にエビデンスを抽出する機能がないことが多く、大量の情報を処理しきれていない可能性があります。産業用ネットワークでの異常なふるまいや不審な対象は、迅速かつ簡単に調査できる必要があります。Cisco SecureX などのプラットフォームでは、Cisco AMP、Umbrella、Stealthwatch、Firepower などを搭載した ISA 3000 や Cyber Vision によって検出された、さまざまなモニター対象を自動的に検索できます。Cisco SecureX はこれらすべての情報源を集約できるため、セキュリティアナリストは、産業用アセットが侵害されているかどうかを即座に確認できます。

また、IT/SecOps チームが簡単にポリシーを設定したり修復したりできるようにするには、すべてのセキュリティツールに OT コンテキストが必要です。たとえば、産業プロセスにおける各アセットの役割、アセットが属する生産セル、パッチを適用できない可能性がある脆弱性などを把握できれば、適切なセキュリティポリシーを作成したり、ファイアウォールのルールを構築したりすることがはるかに容易になります。

効果的に目的を達成できる OT セキュリティ戦略を策定するには、すべての関係者が協力して取り組む必要があります。IT と OT の両方に関連する、産業プロセスの異常と脅威の検出のすべてにメリットがあるようなソリューションでなければなりません。OT 脅威を検出するには、IT と OT を理解する必要があります。脅威は IT 環境から侵入し、OT 環境に拡散する可能性があるからです。セキュリティアナリストがサイバーキルチェーンを特定し、潜在的な脅威を阻止するには、IT と OT の両環境の脅威を検出し、各環境のコンテキストに関する詳細情報を抽出できるツールが必要です。

The bridge to possible

統合された組織と分断された組織

OT 環境には多くの課題がありますが、セキュリティを確保するために重要なのは、部門間を分断している障壁をなくすことです。IT と OT が連携すれば課題を解消できます。OT 向けの新たなセキュリティ手法をばらばらに適用するのではなく、既存のツールと投資を活用して、生産活動を中断することなく OT 環境のセキュリティを強化することが重要です。産業界の企業を保護するためには、既存の IT セキュリティツール（既存のスキル、知識、予算）を OT に拡張し、OT 情報（デバイス、プロセス、イベントなど）と OT エンジニアの知識を IT に取り込むことが必要です。

そのためには、IT/SecOps チームが OT チームと緊密に連携する必要があります。また、すべての関係者とその個別のニーズに対応できるような OT セキュリティソリューションを選択しなければなりません。IT と OT の両方のチームが状況について同じように理解し、共通の目標に向けて協力して進んでいくには、両方のチームに有意義な情報を提供するように最初から設計されたソリューションが必要です。

シスコの支援策

シスコは、サイバーセキュリティと産業用ネットワークの両方の市場におけるリーダーとして、IT と OT をつなぎ、安全に Industry 4.0 を導入するために多額の投資を行っています。

Cisco Cyber Vision とシスコの産業用ネットワーク機器を組み合わせることで、お客様はコンテキストを可視化し、大規模な生産プロセス全体で脅威を検出できます。Cisco SecureX および、シスコのセキュリティ ソリューション スイートと包括的に統合されたソリューションを利用することで、真に統合された IT/OT 脅威管理戦略を実現できます。

詳細については、cisco.com/jp/go/iotsecurity を参照するか、こちらから各地域のシスコ アカウント担当者にお問い合わせください。

C11-744337-00 10/20