Cisco Cyber Vision

© 2024 Cisco and/or its affiliates. All rights reserved.

目次

© 2024 Cisco and/or its affiliates. All rights reserved.

Cisco® Cyber Vision を使用すると、組織は産業用制御システム（ICS）を継続的に可視化して、セキュリティ態勢を把握し、産業用ネットワークの効率を向上させ、IT セキュリティを生産工程に拡張することで、操業の継続性、復元力、安全性を確保できます。

製品の概要

IT、クラウド、産業用ネットワークを緊密に統合するほど、産業用制御システム（ICS）はサイバー攻撃の脅威にさらされることになります。産業のデジタル化への取り組みのメリットを把握し、産業でのモノのインターネット（IIoT）技術の展開を開始する際には、操業の継続性、復元力、および安全性の確保に役立つサイバーセキュリティ ソリューションが必要です。

Cisco Cyber Vision は産業ネットワークを完全に可視化できるように設計されています。OT セキュリティ態勢に関する正確な情報を提供することで、安全なインフラストラクチャを構築し、規制に準拠し、セキュリティポリシーを適用して、リスクを制御できます。

Cisco Cyber Vision は、独自のエッジ モニタリング アーキテクチャと、シスコの主要なセキュリティ ポートフォリオとの緊密な統合を兼ね備えています。シスコの産業用ネットワーク機器に組み込まれているため、大規模な展開が容易にでき、生産設備とそのアプリケーションフローをリアルタイムでモニタできます。IT セキュリティ オペレーション センター（SOC）に OT コンテキストを提供する理想的なソリューションであるため、統合された IT/OT サイバーセキュリティ アーキテクチャを構築できます。

機能と利点

表 1. 機能と利点

機能	利点
独自のエッジアーキテクチャ	OT セキュリティの大規模な展開が容易にできます。Cyber Vision のセンサーは一部のシスコネットワーキング機器に組み込まれているため、専用のアプライアンスを導入したり、アウトオブバンド SPAN 収集ネットワークを構築したりする必要はありません。Cyber Vision を使用すると、サードパーティ製機器で構築された産業トラフィックを簡単にモニタできます。
ゼロタッチプロビジョニング	Cyber Vision センサーの登録を自動化し、大規模なインフラストラクチャを数分で展開します。手動タスクやサービスの中断を行うことなく、センサーを常に最新の状態に保ちます。
ネットワークの過負荷なし	ネットワークリソースを追加する必要はありません。Cyber Vision のセンサーは、エッジで産業用ネットワークトラフィックを復号化し、軽量のメタデータのみを Cyber Vision Center に送信します。この独自のアーキテクチャによって増える産業用ネットワークの負荷はわずか 2 ～ 5% です。
パッシブディスカバリとアクティブディスカバリ	Cyber Vision は、産業用制御プロトコルのディープ パケット インスペクション（DPI）を使用してネットワークトラフィックを受動的にキャプチャおよびデコードすることにより、生産工程を監視します。実行中の特定の ICS プロトコルのセマンティクスで非常に正確で非破壊的な要求を送信するアクティブディスカバリによって、より多くの情報を収集できます。
100% の可視性	産業用ネットワークを 100% 可視化できるのは、Cyber Vision の分散型エッジ アクティブ ディスカバリのみです。ネットワーク機器に組み込まれたセンサーから対象を絞った問い合わせを送信するため、これらのメッセージはファイアウォールやネットワークアドレス変換（NAT）の境界によってブロックされず、100% の可視性が得られます。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
すべてのサイトのグローバルビュー	すべての産業サイトの詳細なセキュリティ情報でガバナンスとコンプライアンスを推進します。Cyber Vision Global Center はすべてのローカルセンターからのデータをシームレスに集約するため、CISO とセキュリティチームは、サイトごとやサイト全体の設備とイベントを一元的に可視化できます。
動的資産台帳	適切なセキュリティポリシーを構築し、運用効率を向上させます。Cyber Vision は生産設備、その通信パターン、およびアプリケーションフローをリアルタイムで詳細に可視化します。
リスクスコアリング	差し迫った脅威に焦点を当て、アクションに優先順位を付けて、セキュリティ態勢を迅速に改善します。Cyber Vision は、各デバイス、特定のサイト、回線、またはデータセットのリスクを計算します。また、リスクをプロアクティブに削減するために何ができるかについてのガイダンスも提供します。
マップビュー	制御ネットワークのアクティビティを可視化します。Cyber Vision では設備とその通信を表示するための複数のタイプのマップを提供しています。カラーコーディングにより脅威や異常をすばやく特定できます。
ゾーンとコンジットの明文化	セキュリティポリシーを簡単に構築できます。Cyber Vision では設備をゾーン（生産セル、建物、変電所など）にグループ化できるため、業務チームは論理ネットワーク情報を IT と共有し、ISA/IEC 62443 に従ってセキュリティポリシーを構築できます。
運用状況の把握	ダウンタイムを減らし、ネットワーク効率を向上させます。Cyber Vision は、すべての OT イベントを監視して、生産が中断される前にデバイスの問題を特定し、保全チームが問題をより迅速にトラブルシューティングできるようにします。問題のあるネットワークパターンを識別して、IT が構成とネットワークパフォーマンスを最適化できるようにします。
OT タグ	各デバイスの役割と何を実行しているかをすぐに理解します。Cyber Vision はアプリケーションフローを人間が読み取れるタグに変換するため、プロトコルのエキスパートでなくても現在の状況を把握できます。
プリセットビュー	事前に設定されたビューとカスタムビューを使用してデータセットを簡単に分析し、重要な情報を強調表示することで、検出戦略に集中し、同僚とターゲット情報を共有できます。
セキュリティに関するインサイト	現在のセキュリティステータスをすばやく理解し、異常や脆弱性を特定し、脅威に対応します。Cyber Vision はセキュリティの問題を簡単に特定し、すべての関係者と情報を共有できるように、さまざまなダッシュボード、レポート、イベント履歴を提供します。
セキュリティ態勢レポート	OT 環境に展開された不正なリモート アクセス ゲートウェイを検出するリモートアクセスレポートなど、産業の業務または事業の特定の部分のセキュリティ態勢に関する詳細なレポートにより、OT セキュリティガバナンスをより適切に推進します。
脆弱性の検出	生産設備を安全に保ちます。Cyber Vision は、パッチを適用する必要があるハードウェアやソフトウェアの脆弱性を警告します。
侵入検知（IDS）	IT ネットワークから発生するサイバーセキュリティの脅威を発見します。Cyber Vision は Talos® サブスクリプションルール（共有オブジェクトルールなど）を活用した Snort IDS エンジンを統合し、マルウェアや悪意のあるトラフィックなどの既知の脅威や新たな脅威を検出します。
異常検出	通常のプロセス動作からの逸脱を検出します。複数のベースラインを簡単に作成して、生産工程をプロファイリングしたり、最も重要なもの（特定の設備や、リモートアクセスなどの特定の動作など）に焦点を当てます。偏差を検出するとすぐにアラートをトリガーします。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
IT/OT セキュリティイベントの関連付け	セキュリティイベント管理の実践を強化します。Cyber Vision は、IBM QRadar や SPLUNK などの主要な SIEM および SOAR プラットフォームと事前に統合されており、Syslog を使用して OT イベントとアラートを他のツールに転送できます。イベント疲弊を回避するため、共有するイベントタイプを選択することもできます。
IT/OT コラボレーション	生産設備とプロセスに関する OT の知識を活用します。Cyber Vision は、IT と OT 間のコラボレーション ワークフローの構築を助長し、生産を効率的に保護します。OT は、追加のコンテキストを提供することでセキュリティイベントを報告できます。IT は OT 設備とグループにカスタムプロパティを追加して、特異性、依存関係、および関係者を文書化できます。
IT セキュリティを OT に拡張	統合された OT/IT SOC を構築します。Cyber Vision はシスコの IT セキュリティ プラットフォーム（およびその他のプラットフォーム）と完全に統合されており、OT 設備とイベントに関する詳細な情報を提供します。既存の IT ツールを使用して OT のセキュリティポリシーを作成し、脅威を修復することがはるかに簡単になりました。
IT との豊かな統合	OT コンテキストを IT ツールと簡単に共有できます。Cyber Vision には、多くのサードパーティソリューション（ファイアウォール、ServiceNow の OT の管理）が事前に統合されており、カスタム統合を構築するための豊富な REST API が備わっています。API Explorer は、使いやすいユーザーインターフェイスを介して API コールを作成およびテストするのに役立ち、ユーザーが作業を開始するためのコードサンプルが付属しています。
オンプレミスまたはクラウド	希望する場所と方法で導入できます。ハードウェアまたは仮想アプライアンスを使用するオンプレミス、またはクラウド内。Cyber Vision は Amazon Web Services または Microsoft Azure にインストールできます。
情報保証とコンプライアンス	FIPS 140-2 モードの Cyber Vision を使用して、組織のデータを保護し、情報セキュリティ標準規格に準拠します。

産業用ネットワークに組み込まれたセキュリティ

Cisco Cyber Vision 独自のエッジ コンピューティング アーキテクチャでは、シスコの産業用ネットワーク機器内にセキュリティ モニタリング コンポーネントが組み込まれています。専用のアプライアンスを調達し、それらをどのように取り付けるかを考える必要はありません。また、産業用ネットワークフローを中央のセキュリティ プラットフォームに送信するアウトオブバンド ネットワークを構築する必要もありません。Cyber Vision は産業用ネットワークが包括的な可視性、分析、脅威の検出を提供するために必要な情報を収集できるようにします。OT セキュリティを大規模に展開する際の Cyber Vision のアーキテクチャの比類のないシンプルさと低コストをネットワークマネージャは実感するはずです。

© 2024 Cisco and/or its affiliates. All rights reserved.

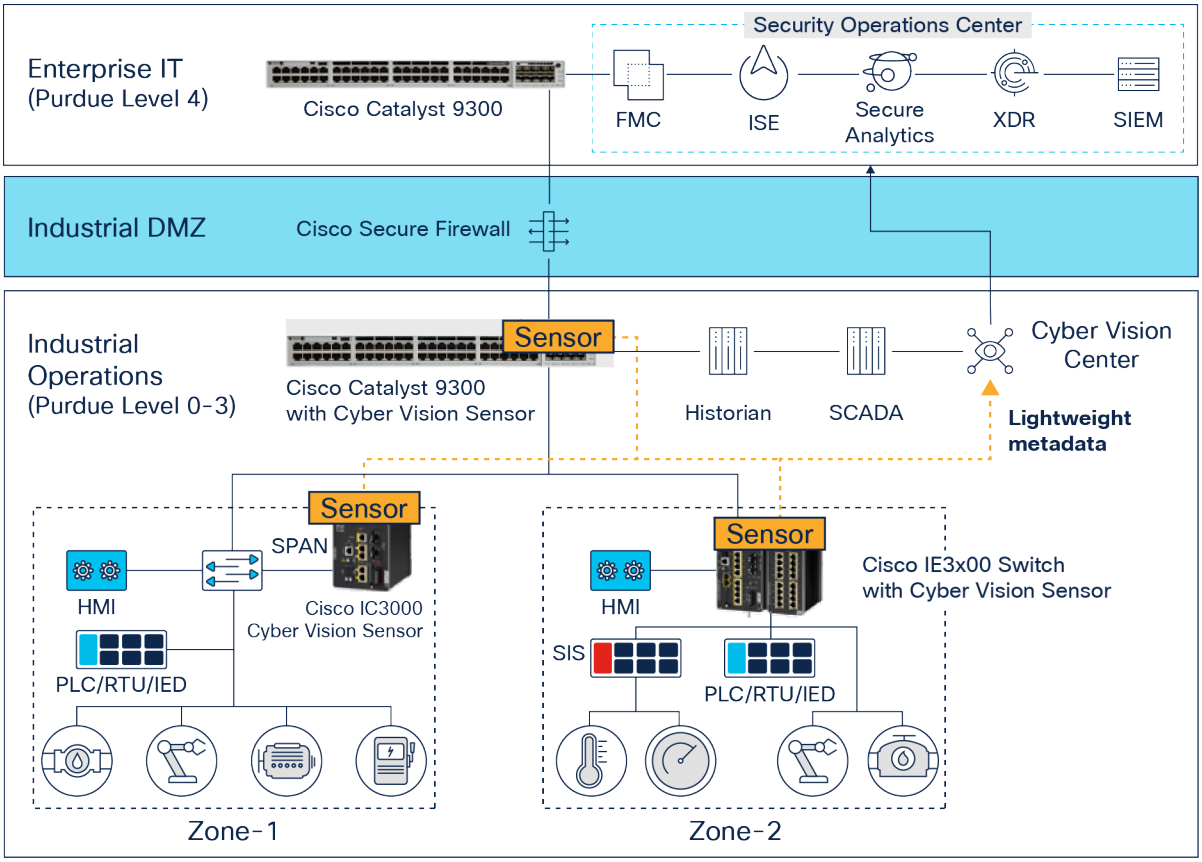

図 1.
Cyber Vision のネットワークセンサーには可視性を大規模に実現する柔軟性が備わっており、ネットワークパフォーマンスに影響を与えることはありません。

包括的な可視性

Cyber Vision は、パッシブディスカバリとアクティブディスカバリのメカニズムを活用して、すべての資産、それら設備の特性および通信を識別します。アクティブ ディスカバリ クエリは極めて正確で非破壊的です。それらは、進行中のプロトコルのセマンティクスを使用して、Windows ベースのシステムを含むすべての産業用資産の詳細を収集します。クエリは、産業用ネットワークを形成するシスコネットワーク機器に組み込まれた Cyber Vision センサーから開始されるため、ファイアウォールや NAT 境界によってブロックされることがなく、包括的な可視性が得られます。

設備、通信マップ、運用およびセキュリティイベントに関するこの豊富な情報には、ローカルの OT チームと IT チームのメンバーがアクセスできます。また、Cyber Vision Global Center 内に集約することで、大規模な組織ではすべてのサイトにわたるグローバルな可視性を得て、ガバナンスとコンプライアンスを推進することもできます。

© 2024 Cisco and/or its affiliates. All rights reserved.

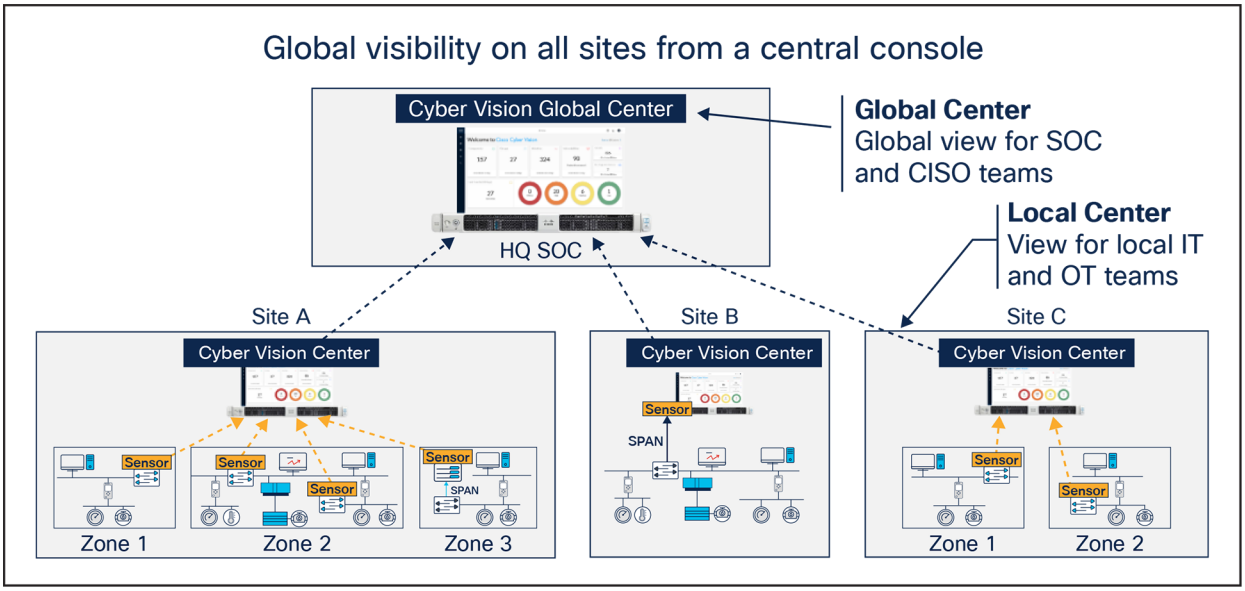

図 2.
Cyber Vision は非侵襲型のエッジアーキテクチャを活用して、ローカルやグローバルの関係者に詳細な情報を提供します。

セキュリティ態勢

Cisco Cyber Vision は、プロトコル分析、侵入検知、脆弱性検知、および動作分析を組み合わせて、セキュリティ態勢の把握を支援します。各コンポーネント、デバイス、および生産工程の特定の部分のリスクスコアを自動的に計算して、重要な問題を強調表示するため、修正が必要なものに優先順位を付けることができます。各スコアには、リスクに対処するためにプロアクティブに改善プロセスを構築できるように、リスクを軽減する方法に関するガイダンスが付属しています。

Cyber Vision の検出エンジンは、世界有数のサイバーセキュリティ研究チームの 1 つであり、Snort シグネチャファイルの公式開発者である Cisco Talos の脅威インテリジェンスを活用します。Cyber Vision 脅威ナレッジベースは毎週更新され、設備の脆弱性や IDS シグネチャの最新のリストを組み込みます。

運用状況の把握

Cisco Cyber Vision は、ベンダーの詳細、ファームウェアとハードウェアのバージョン、シリアル番号、ラックスロットの設定など、実稼働インフラストラクチャの些細な詳細を自動的に発見し、設備の関係性、通信パターンなどを特定します。情報は、さまざまなタイプのマップ、テーブル、およびレポートに表示されます。

Cisco Cyber Vision は予期しない変数の変更やコントローラの変更などの生産プロセスの実際のステータスに関するリアルタイムのインサイトを OT エンジニアに提供します。そのため、製造における問題を迅速にトラブルシュートし、稼働時間を維持することができます。サイバーエキスパートは、容易にこれらすべてのデータを調べて、セキュリティイベントを調査できます。インシデントレポートを文書化し、法令遵守を推進するために必要なすべての情報が最高情報セキュリティ責任者に提供されます。

製品はタグを使用して設備の役割と通信コンテキストを強調表示するため、OT や IT のチームメンバーは設備のブランドや参照情報に関係なく、産業インフラストラクチャと運用イベントを容易に理解できます。IT チームは OT スタッフと連携して、脆弱な設備へのパッチ適用、デフォルトパスワードの使用状況の追跡、ネットワーク セグメンテーションの改善などのベストプラクティスを推進できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

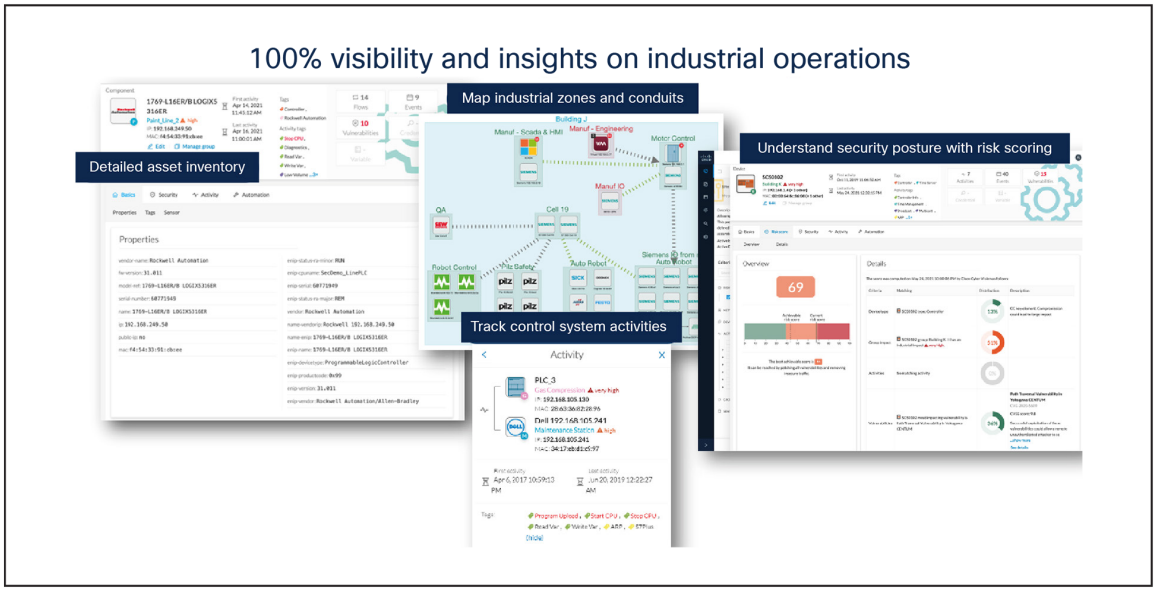

図 3.
設備、生産プロセス、通信フロー、セキュリティ態勢に関する運用上のインサイトの獲得

IT セキュリティの統合

Cyber Vision の詳細な資産台帳と OT イベントの可視性は、業務チームと IT セキュリティチームの両方に価値をもたらします。シスコのセキュリティポートフォリオに留まらない広範なサードパーティ製ソリューションのすぐに利用可能な統合により、リスクや遵法監視とレポート作成、セキュリティポリシーの適用その他に対する Cyber Vision のインサイトが拡張されます。また、IT SOC を OT ドメインに拡張します。

Cyber Vision は主要な SIEM システム（IBM QRadar、SPLUNK など）とシームレスに統合できるため、セキュリティアナリストは既存のツールで産業イベントを追跡し、OT/IT イベントの関連付けを開始できます。Cyber Vision の豊富な API を活用することで、IT チームと OT チームは、生産設備、ネットワークトラフィック、セキュリティ態勢に関する深い知識を既存のツールに対して提供できます。

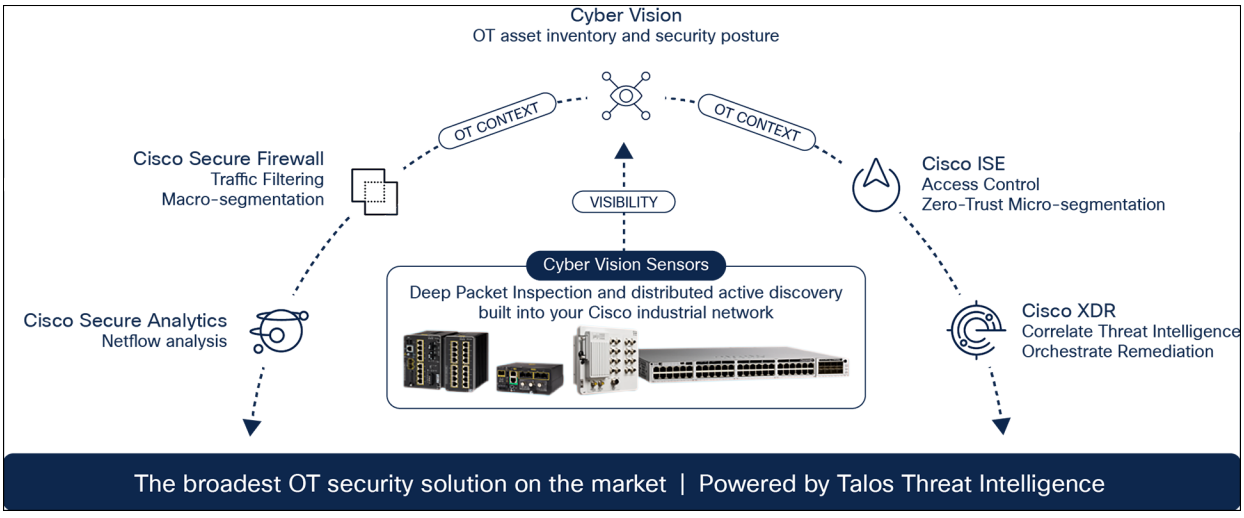

図 4.
Cyber Vision は、既存のツールに生産設備とイベントのコンテキストを提供することで、IT セキュリティ運用を OT に拡張します。

© 2024 Cisco and/or its affiliates. All rights reserved.

Cisco XDR

Cisco Cyber Vision に異常な振る舞いが見られますか。[Report to XDR] ボタンをクリックするだけで Cisco XDR にケースが作成され、アナリストが特定のプレイブックやカスタムワークフローを使用して調査し、修復を開始できます。Cyber Vision のユーザーインターフェイスで常に使用可能な XDR リボンにより、修復ワークフローをこれまで以上に簡単にトリガーし、脅威を迅速に封じ込めます。リボンでは、Cyber Vision が検出したすべての観測可能データ（IP/MAC アドレス、ユーザー名、ホスト名、URL など）が強調表示されるため、OT コンテキストを使用して XDR に簡単に視点を移し、詳細な調査を開始できます。Cisco XDR は、Cisco Secure Endpoint、Cisco Secure Network Analytics、Cisco Secure Firewall、Umbrella、Talos インテリジェンスフィード、およびその他の接続テクノロジー（シスコおよびサードパーティ製）のインテリジェンスを活用して、IT および OT ネットワーク全体の脅威とアクティビティを完全に把握します。

Cyber Vision と Cisco XDR の連携の詳細については、ソリューションの概要をご覧ください。

Cisco Secure Firewall

ネットワーク セグメンテーションは、ネットワークを安全に保ち、重要なプロセスを保護するための重要な柱です。Cyber Vision は、制御エンジニアが作成した設備グループを Firewall Management Center（FMC）と共有し、Cisco Secure Firewall によって管理されるアクセス制御ポリシーに影響を与え、産業用ネットワーク内の通信を制限できます。OT 設備グループは動的オブジェクトとして Cisco Secure Dynamic Attribute コネクタ（CSDAC）を介して共有されるため、Cyber Vision で行われた変更は FMC に自動的に反映され、面倒な手動更新やポリシー展開を行うことなくルールを最新の状態に保ちます。

Cisco Secure Firewall ポリシーでの動的属性の使用の詳細については、このドキュメントをご覧ください。

Cisco Identity Services Engine（ISE）

ソフトウェアベースのネットワーク セグメンテーション ポリシーを産業用制御ネットワークに拡張し、ゼロトラストセキュリティの適用を開始します。Cyber Vision は、検出されたホスト、プロトコル、通信パターンなどを、pxGrid を通じて Cisco ISE と共有し、ISE の認識とポリシー適用を制御ネットワークに拡張します。Cisco ISE は、Cyber Vision の制御エンジニアが作成した設備グループを活用して、セキュアゾーンを自動的に構築し、産業用ネットワークの動的なマイクロセグメンテーションを推進することもできます。設備を Cyber Vision の別のグループに移動するだけで、この設備に対応するセキュリティポリシーが ISE に自動的に適用されます。

Cyber Vision と ISE の連携の詳細については、ソリューションの概要をご覧ください。

Cisco Secure Network Analytics

ネットワーク インフラストラクチャからテレメトリを調べることで、振る舞い分析を拡張します。Cisco Secure Network Analytics は Cyber Vision のインサイトを使用して監視対象のネットワークフローにコンテキストを追加し、アラームでの ICS 設備を特定することでインシデント対応とフォレンジックを高速化します。

REST API

Cyber Vision は、REST API を介して機能とデータアクセスを公開します。これにより、コンプライアンスおよびリスクレポートの作成、システムおよびイベントの監視とダッシュボードなどのために、サードパーティ製アプリケーションと自社製アプリケーションのカスタム統合が可能になります。組み込みの API Explorer には独自の API コールを作成し、それらをテストし、コードを簡単に生成するための使いやすいユーザインターフェイスが備わっています。ServiceNow OT 管理など、すぐに使用できる統合を利用できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

Common Event Format（CEF）

Cyber Vision の検出およびイベントデータは、SIEM ソリューション、セキュリティ オーケストレーション、自動化、および対応（SOAR）のプラットフォームなどの任意の数のサードパーティ製アプリケーションで使用するために、Common Event Format（CEF）syslog で出力できます。IBM QRadar および Splunk OT と簡単に統合できる無料のアドオンを利用できます。

プラットフォームのサポート

Cisco Cyber Vision は産業用ネットワーク内のディープ パケット インスペクション、プロトコル分析、および侵入検知を実行する複数のセンサーデバイスと、Cyber Vision Center として知られる集約プラットフォームで構成される、独自のエッジアーキテクチャ上に構築されています。Cyber Vision Center はセンサーからのデータを保存し、ユーザインターフェイス、分析、振る舞い分析、レポート作成、API などを提供します。ハードウェアアプライアンスで実行することも、仮想マシンとして実行することもできます。センサーは次の表に示すプラットフォームでサポートされています。

表 2. Cyber Vision 製品のプラットフォーム

製品コンポーネント	サポートされているプラットフォーム
ハードウェア センサー アプライアンス	Cisco IC3000 産業用コンピューティング ゲートウェイ [英語]（IC3000-2C2F-K9）
ネットワークセンサー	Cisco Catalyst® IE3300 高耐久性シリーズ スイッチ（4 GB RAM 搭載モデルのみ） Cisco Catalyst IE3400 高耐久性シリーズ スイッチ Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ Cisco Catalyst IE9300 高耐久性シリーズ スイッチ Cisco Catalyst IR1100 高耐久性シリーズ ルータ Cisco Catalyst IR1800 高耐久性シリーズ ルータ Cisco Catalyst IR8300 高耐久性シリーズルータ Cisco Catalyst 9300 および 9300X シリーズスイッチ Cisco Catalyst 9400 シリーズ スイッチ Rockwell Stratix 5800 スイッチ
センターのハードウェアアプライアンス	Cisco UCS C225 M6N ラックサーバー [英語]（CV-CNTR-M6N 構成）
センターのソフトウェアアプライアンス	VMware ESXi ソフトウェアアプライアンス Microsoft Hyper-V ソフトウェアアプライアンス Amazon AWS ソフトウェア アプライアンス Microsoft Azure ソフトウェア アプライアンス

© 2024 Cisco and/or its affiliates. All rights reserved.

Cyber Vision センサーハードウェアの仕様

ハードウェアの仕様については、関連するデータシートを参照してください。

- Cisco IC3000 産業用コンピューティング ゲートウェイ [英語]
- Cisco Catalyst IE3300 高耐久性シリーズ スイッチ
- Cisco Catalyst IE3400 高耐久性シリーズ スイッチ
- Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ
- Cisco Catalyst IE9300 高耐久性シリーズ スイッチ
- Cisco Catalyst IR1100 高耐久性シリーズ ルータ
- Cisco Catalyst IR1800 高耐久シリーズ ルータ
- Cisco Catalyst IR8300 高耐久性シリーズルータ
- Cisco Catalyst 9300 および 9300X シリーズスイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Rockwell Stratix 5800 スイッチ

Cyber Vision Center ハードウェアアプライアンスの仕様

表 3. Cyber Vision Center ハードウェアアプライアンスの仕様

項目	CV-CNTR-M6N
フォーム ファクタ	1RU Cisco UCS C225 M6N ラックサーバー
プロセッサ	AMD 2.85 GHz 7443P（24 コア）
メモリ	16GB RDIMM SRx4 3200MHz X 8
RAID	ソフトウェア対応 RAID は、ドライブの数に応じて RAID 1 または RAID 10 を提供します。
内蔵ストレージ	1.6 TB NVMe Extreme Perf. X 2 または X 4 高耐久性ドライブ
組み込みネットワーク インターフェイス カード（NIC）	デュアル 10GBASE-T Intel x710 イーサネットポート
電源装置	ホットプラグ可能、ラックサーバー用 Cisco UCS 1050W AC 冗長電源
管理	Cisco Intersight™ Cisco Integrated Management Controller (IMC) Cisco UCS Manager
ラック オプション	Cisco ボール ベアリング レール キットまたはフリクション レール キット（オプションのリバーシブル ケーブル管理アーム）

その他のハードウェア仕様については、Cisco UCS C225 M6N ラックサーバー のデータシートを参照してください。

© 2024 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Center ハードウェアアプライアンスのパフォーマンス

表 4. Cisco Cyber Vision Center （スタンドアロン/ローカル）ハードウェアアプライアンスのスケール

項目	CV-CNTR-M6N
コンポーネントの最大数	50,000
センサーの最大数	300
保存されるフローの最大数	1600 万

表 5. Cisco Cyber Vision Global Center のスケール

項目	CV-CNTR-M6N
同期可能なコンポーネントの最大数	150,000
登録可能なセンターの最大数	20

Cyber Vision Center 仮想アプライアンスの仕様

表 6. Cyber Vision Center 仮想アプライアンスの最小仕様*

特性	プライベートクラウド	パブリッククラウド
CPU	Intel Xeon、10 コア	Intel Xeon、10 コア
メモリ	最小 32 GB	最小 32 GB
ストレージ	最小 1 TB SSD	最小 1 TB SSD
仮想ソフトウェア	• VMware ESXi 6.x 以降 • Windows Server 2016 以降の Microsoft Hyper-V	• Amazon Web Services • Microsoft Azure

*これらの VM 要件は、最大 10000 のエンドポイントのモニタリングをサポートします。

Cisco Cyber Vision Center 仮想アプライアンスは、software.cisco.com から直接ダウンロードできます。

© 2024 Cisco and/or its affiliates. All rights reserved.

ライセンス

Cisco Cyber Vision は、監視対象のエンドポイントの数に基づいた定期的なサブスクリプションモデルを使用してライセンスが供与され、1 年、3 年、5 年、および 7 年の期間で利用できます。ライセンスは、特定の要件を満たすためのさまざまなレベルの機能を提供する 2 つの階層（Essentials と Advantage）で使用できます。製品は、エアギャップネットワーク用の特定のライセンス予約（SLR）ライセンスのオプションとともに Cisco Smart Licensing を使用します。現在のサブスクリプション ライセンスには、Cyber Vision Center とセンサーソフトウェアへのアクセスが含まれます。これらのソフトウェアは、software.cisco.com から直接ダウンロードできます。

表 7. ライセンス階層

ライセンスレベル	
Essentials	**Advantage**
インベントリ • デバイスインベントリ • 通信パターンの特定 • インベントリレポートの生成 **脆弱性** • デバイスの脆弱性の特定 • 脆弱性レポートの作成 **アクティビティ** • 制御システムのイベントの追跡 • デバイス アクティビティ レポートの生成 **RESTful API** • REST API プログラミング インターフェイス	Essential 機能の他以下を搭載 **セキュリティ態勢** • デバイスリスクの評価 • セキュリティ態勢レポート **侵入検知（IDS）** • サポートされているセンサーの Snort IDS • Talos コミュニティの署名（新しいルールはリリースから 30 日後に追加される可能性があります） **ふるまいモニタリング** • 設備のふるまいに対するユーザー作成ベースライン • 逸脱に関するアラート **高度な統合** • Cisco XDR リボン • ISE との pxGrid の統合 • Firepower ホスト属性の統合 • SIEM 統合：Splunk、IBM QRadar • ServiceNow OT 管理の統合
	Cyber Vision IDS の Talos サブスクライバ ルール オプション
	（Cyber Vision Advantage が必要です。IDS センサーごとにライセンスが必要です） • Talos サブスクリプション シグニチャ（特に産業用ネットワーク向けに管理されているもの） • すぐに利用できるルールの可用性 • コミュニティ署名と比較して 15 倍のルール

エンドポイント ライセンス パックは、必要な任意の数のエンドポイントで使用できます。IDS は、Cyber Vision、Cisco IC3000 ハードウェアセンサー、Catalyst IR8300 Rugged ルーター、および Catalyst 9300、9300X または 9400 スイッチで利用できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

発注情報

Cisco Cyber Vision は現在注文可能です。詳細については、シスコの購入案内のページを参照してください。

表 8. Cyber Vision の製品 ID

製品 ID	製品の説明
CV-LICENSE	Cyber Vision サブスクリプション ライセンス
CV-CNTR-M6N	Cyber Vision Center ハードウェアアプライアンス（Cisco UCS C225 M6N ラックサーバー）
IC3000-2C2F-K9	Cyber Vision Sensor ハードウェアアプライアンス（Cisco IC3000 産業用コンピューティング ゲートウェイ）
CV-IDS-CNTR	Cyber Vision Center IDS（ハードウェアおよび仮想アプライアンス）の Talos サブスクライバ ルール ライセンス
CV-IDS-IC3000	IC3000-2C2F-K9 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ライセンス
CV-IDS-IR8300	Catalyst IR8300 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ライセンス
CV-IDS-C9000	Catalyst 9300/9300X/9400 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ライセンス

保証情報

保証情報については、IC3000 産業用コンピューティング ゲートウェイと Cisco UCS C225 M6N ラックサーバーのそれぞれのデータシートを参照してください。

シスコの環境保全への取り組み

持続可能性に関する情報については、IC3000 産業用コンピューティング ゲートウェイと Cisco UCS C225 M6N ラックサーバーのそれぞれのデータシートを参照してください。

シスコおよびパートナーの提供サービス

計画、展開、およびサポートのためのサービス

シスコとシスコの認定パートナーが提供するサービスは、お客様の Cisco Cyber Vision プロジェクトの評価、設計、展開、運用の各フェーズでご利用いただけます。必要とされているのがエキスパートのアドバイスでもプロジェクト全体のサポートでもその間の何らかのサポートでも、シスコはパートナーとともにお客様の成功を支援するエキスパートと専門知識を提供できます。詳細については、https://www.cisco.com/go/services [英語] を参照してください。

© 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切な技術を簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、および他社製製品を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
Catalyst IE9300 高耐久性スイッチ、FIPS 準拠に対するサポートを追加	バージョン 4.1.4	2023 年 1 月
可視性機能とその他の可用性に関する詳細を追加	バージョン 4.2	2023 年 4 月
UCS M6、Catalyst 9300X スイッチ、および新機能のサポートを追加	バージョン 4.3	2023 年 11 月
UCS M5 を削除。Cisco XDR および FMC CSDAC のサポートを追加	バージョン 4.4	2024 年 4 月
Catalyst IR1800 高耐久性ルータおよび ZTP のサポートを追加	バージョン 5.0	2024 年 7 月

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

Printed in USA C78-743222-07 07/24

© 2024 Cisco and/or its affiliates. All rights reserved.