データシート
Cisco Public

Cisco XDR

セキュリティ運用を簡素化

2025 年 5 月

目次

Cisco XDR 製品の概要

セキュリティ運用を簡素化

Cisco XDR は、セキュリティ運用を簡素化し、対応を迅速化し、セキュリティ オペレーション センター（SOC）チームに AI 主導型のプロアクティブな脅威検出および対応能力を提供します。また、セキュリティアナリストが直面する課題に対処するように設計されており、複数のセキュリティツールからデータを取得し、機械学習と分析を適用して相関検出を実現するクラウドネイティブで拡張可能なソリューションを提供します。

Endpoint Detection and Response（EDR）やセキュリティ情報イベント管理（SIEM）中心のアプローチから、Cisco XDR は、無限の調査から自動化に基づく証拠による最も優先度の高いインシデントの修復に焦点を移し、SOC チームが速度、効率、および信頼性をより高めて行動できるようにします。従来の SIEM テクノロジーは、ログ中心のデータの管理を提供して数日で結果を測定しますが、Cisco XDR は、テレメトリ中心のデータに焦点を当てて、数分で結果を提供します。

Cisco XDR は、セキュリティ オペレーション センター（SOC）のオペレータが Extended Detection and Response（XDR）ソリューションに不可欠であると示す 6 つのテレメトリソース（エンドポイント、ネットワーク、ファイアウォール、電子メール、アイデンティティ、および DNS）をネイティブに分析し、関連付けます。Cisco XDR により、セキュリティチームは、ネットワークを含む他のソースからのテレメトリとインサイトを同様に基礎として、エンドポイントを超える脅威を検出できます。サードパーティのセキュリティ製品および広範なシスコのセキュリティ ソリューション ポートフォリオとの厳選された統合により、Cisco XDR は既存のアーキテクチャにシームレスなインストールを行い、ベンダーやソリューションに関係なく一貫した結果を提供します。

Cisco XDR は、データを集約するだけでなく、テレメトリを関連付けます。これにより、誤検出が減少し、環境に対する潜在的なリスクと影響に基づいて、優先順位付けされたインシデントが提供されます。つまり、チームは重要な脅威に集中できます。また、Cisco Talos の脅威インテリジェンスで検出機能を強化し、コンテキストとアセットのインサイトを追加して、全体像を常に把握できるようにします。

XDR を正しく行うことで、セキュリティチームは攻撃に確実に対応し、SOC 効率を向上させ、タスクを自動化してセキュリティに対してよりプロアクティブにアプローチすることができます。

Cisco XDR は、次の 4 つのキー値の柱を通じて、既存のセキュリティスタックからより優れた有効性、より優れたエクスペリエンス、より高い投資回収率（ROI）を実現するように設計されています。

1. 最も高度な脅威の検出：広範なエンドツーエンドのシスコのセキュリティポートフォリオと、さまざまなサードパーティのセキュリティツールを接続することで、環境のあらゆる場所を調査できます。また、Cisco Talos から基盤となる脅威インテリジェンスを提供し、追加されたコンテキストとアセットのインサイトでインシデントを強化することで、ベンダーやベクトルに関係なく、幅広いセキュリティスタックに影響を与える最も高度な脅威を検出して対応できます。
2. 本当に重要な問題に対するより迅速な行動：ビジネスに最も重大なリスクをもたらす脅威を優先順位付けします。調査を合理化するためのコンテキストと証拠に基づいた推奨事項を統合します。
3. 生産性の向上：ノイズを排除して、アナリストが本当に重要な問題に集中できるようにします。限られたリソースを最大値に高めます。タスクを自動化し、戦略的なタスクに集中します。

4. セキュリティレジリエンスの構築：セキュリティギャップを解消します。実用的なインテリジェンスによって次に何が起こるかを予測します。定量化が可能な改善が継続的に行われることで、日々強力になります。

詳細については、cisco.com/go/XDR を参照してください。

使用例

ワークフローの合理化と優先順位付けによるインシデント対応の加速

お客様に代わって調査プロセスを実施することで、Cisco XDR はレベル 1 およびレベル 2 アナリストの作業負担を排除し、インシデント対応をすぐに開始できるようにします。次に、Cisco XDR は、発生したインシデントに基づいて実行する適切な対応に関する明確なガイダンスを提供します。それによって、アナリストはすぐに行動して、環境におけるさらなる影響を防止し、インシデントを解消できます。最後に、それぞれの MITRE ATT&CK の戦術、手法、手順（TTP）に関連付けられた組織にとっての重大なリスクと、影響を受けるアセットの価値に基づいてインシデントの優先順位を付けることにより、Cisco XDR は、組織が潜在的に最も影響の大きいインシデントに確実に焦点を当てることができます。

組み込みの自動化（ローコード/ノーコードのカスタマイズ）

応答のない検出では不十分であるため、応答機能を XDR ソリューションに組み込む必要があります。この標準を強化するため、Cisco XDR には専門家が厳選した自動化とオーケストレーションが含まれており、自動化されたワークフローに対応機能を拡張し、SOC チームやアナリストが必要とする労力を削減します。Cisco XDR によってすぐに使用できる組み込みの機能を拡張する必要がある場合、組織は特定の SOC プロセスを実行するためにカスタマイズされたワークフローを作成して保存できます。ワークフローは、ローコード/ノーコードエディタでドラッグ アンド ドロップ アクションを使用して構築できます。ワークフローは、ガイド付きのハンドブック、自動化ルール（インシデント、電子メール、ウェブフック、スケジュールの各トリガーを使用）などの方法でトリガーされます。

真に拡張された検出と対応の実施

考えられるベクトル、セキュリティデータソース、セキュリティに関連しないデータソース、および対策のすべてにわたって評価していない場合、環境に対するインシデントと脅威をどのように評価できるか？Cisco XDR は、エンドポイント、電子メール、クラウド、ネットワークの主要なベクトルに、シスコのセキュリティソリューションおよびシスコ以外のツールとのネイティブ統合を提供します。Cisco XDR は、エンドポイント、電子メール、クラウド、ファイアウォール、およびネットワークにおける市場をリードするサードパーティのセキュリティ対策のために、これらの主要パートナーとの確立された開発契約を通じて、シスコが厳選した統合を提供および維持することで、お客様の組織が必要とする要件をオフロードし、テクノロジーへの投資を十分に活用します。

環境全体の検出カバレッジの評価

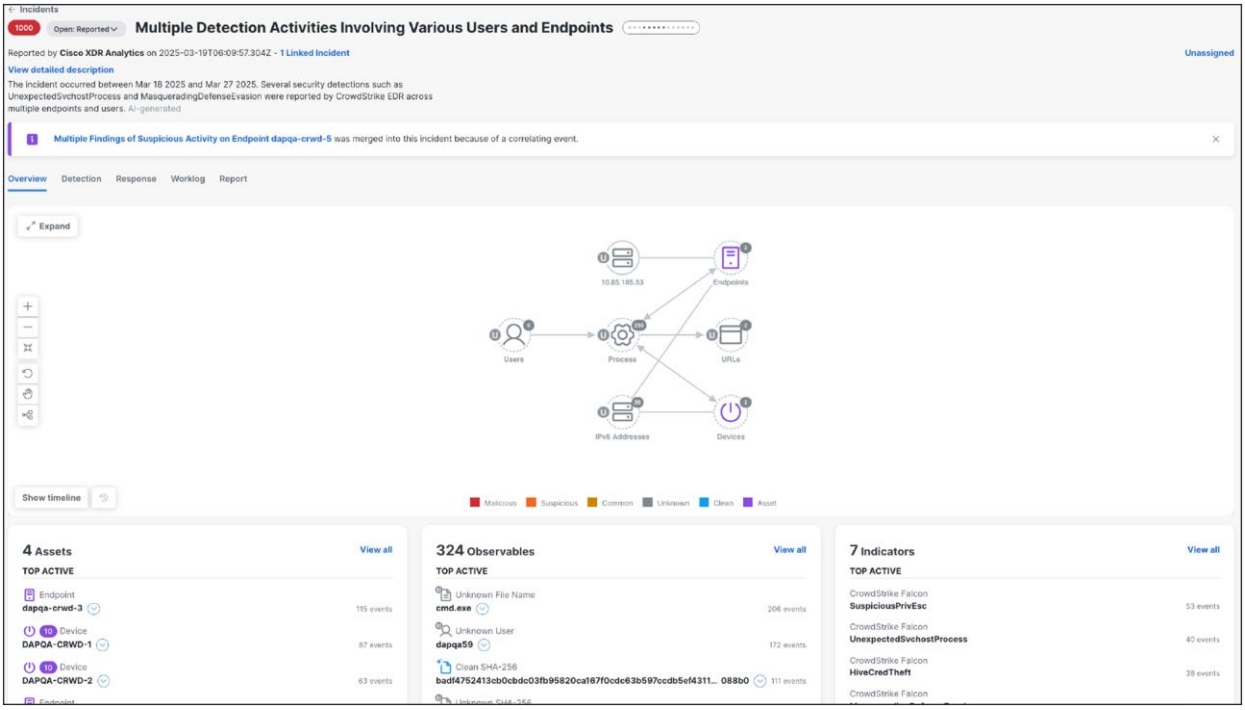
Cisco XDR は、ツールの組み合わせから、および選択した攻撃的な MITRE の手法と戦術に対して、検出カバレッジのシナリオをモデル化することで、業界標準のフレームワークである MITRE ATT&CK に関して、Cisco XDR および関連する統合製品によって提供されるカバレッジ量を評価するのに役立ちます。選択された統合の場合、Cisco Secure Endpoint から開始すると、現在の動的設定と、それがソリューションの全体的なカバレッジに与える影響も評価できます。Cisco Secure Endpoint 設定インサイトにより、関連する製品機能を有効にしているか、無効のままにしているかに基づいて、可視性が得られる MITRE の手法と戦術に関する実用的なイン

サイトを受け取ります。ベストプラクティスに対する継続的な評価を提供し、構成を最適化して MITRE カバレッジを向上させるために確認および調整する必要があるエンドポイントとポリシーを強調表示します。

主要機能

セキュリティ分析と関連付け

Cisco XDR には、さまざまなイベントおよびテレメトリを取り込むことができる分析および相関エンジンが組み込まれています。この範囲は、たとえば、EDR セキュリティイベントからパブリッククラウドおよびプライベート ネットワーク フロー ログまでです。シスコとサードパーティの両方のデータを Cisco XDR に取り込むことができます（ライセンス階層に応じて）。



この分析エンジンは、さまざまな検出および相関メカニズムに基づいて完全に相関するインシデントをユーザーに提供します。セキュリティイベントが時間の経過とともに関連付けられ、多段階の攻撃の全体像が明らかになります。インシデントアクティビティがタイムラインにプロットされ、攻撃グラフによって可視化されるため、アナリストは、誰が、何を、どこで、いつ攻撃されたかをすばやく理解できます。インシデントには、検出に関連するリスクを反映する 1 から 1000 までのスケールの優先スコアが割り当てられます。このリスクは、それぞれの MITRE ATT&CK TTP に関連する重大なリスクと、影響を受けるアセットの価値に関連しています。また、このインシデントは、MITRE ATT&CK フレームワークにマッピングされた攻撃全体を示すために、共通のインジケータに基づいて関連するアラートを関連付けます。

ネットワークテレメトリの取り込み

セキュリティ運用チームは、プライベートネットワーク上のユーザーデバイスの数が増加し、より多くのワークロードがパブリッククラウドに移行するにつれて、環境内で「盲点」に直面することがよくあります。多くの攻撃では、攻撃者は目的を達成するためにネットワークと対話する必要があります。Cisco XDR により、オンプレミスネットワークまたはパブリッククラウドからネットワークトラフィックを収集してホストを識別し、通常のホスト動作を把握し、デバイスの動作が組織のネットワークセキュリティに関連する方法で変化したときにアラートを生成することができます。これらのアラートはその後、インシデント相関プロセスにフィードし、攻撃

チェーンに使用されます。Cisco XDR では、ネイティブ検出のほとんどが MITRE TTP にマッピングされており、調査結果を理解して対応するための業界標準の方法を提供します。

Cisco XDR は、ワークロードと API 統合のエージェントレスの監視を使用して、パブリッククラウドのログ（AWS、Google Cloud プラットフォーム、および Microsoft Azure）を取り込んで、脅威検出と設定の監視を提供できます。また、ネットワーク上の攻撃者の動作を検出し、組織のクラウド環境に深く侵入するために、追加のクラウド サービス プロバイダー API（VPC フローログ、Cloud Trail、Cloud Watch、Config、Inspector、Identity and Access Management（IAM）Lambda などの AWS で）と統合されます。

オンプレミスネットワークを監視するために、Cisco XDR には **XDR コネクタ**（旧 Secure Cloud Analytics センサー/ONA）が含まれています。これにより、フローデータ（NetFlow、IPFIX など）、SPAN/ミラーポートトラフィック、および NGFW ログ情報などの多くのソースからネットワークテレメトリを取り込むことができます。XDR コネクタは、オンプレミスのネットワークテレメトリを SaaS ベースのデータリポジトリに送信し、このデータが保存および分析され、他の利用可能なすべてのテレメトリと関連付けられます。または、**Cisco Telemetry Broker**（CTB）を購入して、ネットワークテレメトリを Cisco XDR やその他のダウンストリームのコンシューマに転送することもできます。

Cisco XDR には、クラウド管理の Cisco Secure Client（旧 AnyConnect）を使用して直接展開できる **Network Visibility Module**（NVM）も含まれています。NVM は、価値の高いエンドポイントテレメトリを継続的に提供します。それにより、組織はネットワーク上のエンドポイントとユーザーの動作を確認できます。ユーザー、アプリケーション、デバイス、場所、接続先などの貴重なコンテキストとともに、オンプレミスとオフプレミス両方のエンドポイントからフローログを直接収集します。NVM テレメトリは、ネットワークテレメトリとエンドポイントプロセス情報を関連付ける際に重要です。これは、1 つのログ行に両方が含まれているためです。

アセットコンテキスト

Cisco XDR Asset Insights 機能は、統合フレームワークを拡張して、デバイスとユーザーのインベントリおよびポスチャに関するデータを収集します。セキュリティ製品と従来のデバイスマネージャからのデータを独自に組み合わせることにより、統合されたアセットインベントリが実現します。これを使用して、調査のコンテキストと意味のあるレポートを提供できます。各アセットには、すべてのソースから統合された、そのアセットに関する情報が 1 ページあります。また、XDR インシデントのスコアリング時に使用されるアセットの「値」を定義することもできます。インシデントにアセットが含まれている場合は、インシデントを確認、調査、および対応する際に表示されます。

Cisco Asset Insights for Devices は Cisco XDR Integrations から直接ソースを利用しますが、Asset Insights for Users は Cisco Security Cloud Control を介して Cisco Identity Intelligence（CII）ソースをネイティブに活用します。Cisco XDR は、CII から相関データを受信し、ユーザーインサイト内に表示します。このメカニズムにより、追加のアイデンティティ プロバイダー（IDP）をソースとして含めることができ、Cisco XDR で活用する新しいアイデンティティ セキュリティ イベントを追加できます。

カスタム自動化のワークフロー

Cisco XDR 自動化は、自動ワークフローを構築するためのノーコード/ローコード アプローチを提供します。これらのワークフローは、シスコまたはサードパーティベンダーかにかかわらず、さまざまなタイプのリソースやシステムと連携できます。自動化ワークフローは親コンポーネントであり、従来のプログラミングのスクリプトに似ています。一方、アトミックアクションは従来のプログラミングの関数に似た再利用可能な構成要素を提供

します。多くの設定済みのワークフローとアトミックを使用できます。ただし、ユーザーはこれらをカスタマイズしたり、グラフィカル ユーザー インターフェイスを使用して独自に作成したりすることもできます。ワークフローは、単純で少数のアクションしか持たない場合もあれば、複雑でさまざまな製品の多くの異なるアクションを結合する場合もあります。ドラッグ アンド ドロップ インターフェイスを使用して、独自のワークフローを作成できます。このワークフローは、さまざまなスケジュールやイベントによってトリガーできます。例としては、新しいインシデント、インシデントステータスの変更、受信した電子メールやウェブフック、スケジュールなどがあります。自動化ルールを使用すると、すべてのワークフローとトリガーを単一の包括的な操作で管理できます。

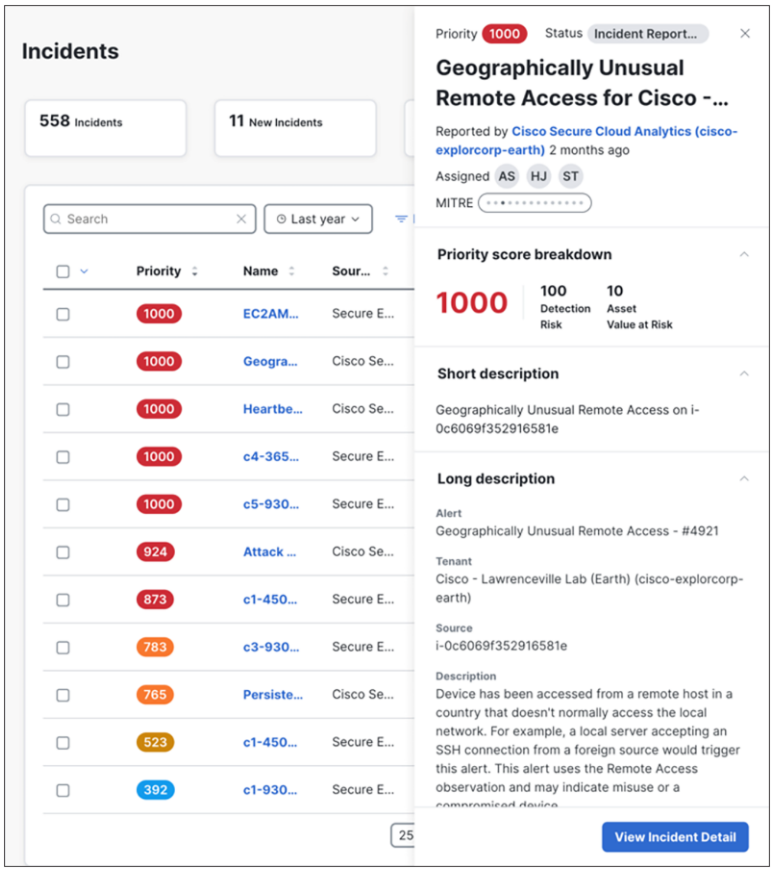
自動化ワークフローの交換

Cisco XDR Automation Exchange を使用すると、新しい自動化ワークフローをすばやく見つけ、インストールウィザードを使用してそれらをインストールして新しく厳選したコンテンツをすばやく検出し、数回のクリックでワークフローを操作可能にすることができます。[交換（Exchange）] ページでは、有用なワークフローを簡単に見つけ、ワンクリック インストール ウィザードを使用してワークフローのインポートプロセスを合理化できます。製品で Exchange をフィルタリングしたり、一般的なワークフローを表示したりできます。

インシデントの優先順位付け

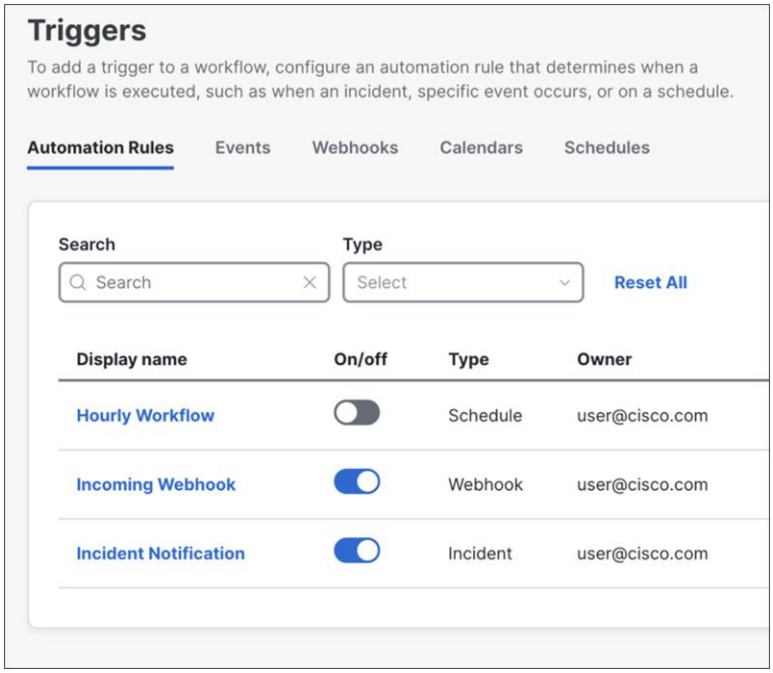
新しいインシデントには優先順位スコアが割り当てられ、自動的に強化されます。インシデントに関連する、エンリッチメントプロセスで検出される新しい検出は、そのインシデントに追加されます。インシデントの優先順位付けに使用されるインシデントの優先順位スコア（1 ～ 1000）は、検出リスク（1 ～ 100）とアセット値（1 ～ 10）で構成されます。検出リスクスコアは、MITRE TTP の財務リスク、MITRE TTP の数、およびソースの重大度で構成されます。アセット値は、インシデントに関連するアセットの値を表すユーザー定義の値です。

インシデントが優先順位付けされると、優先順位スコア順に並べ替えられたリスト形式で表示されるため、アナリストは最初に調査するべきものを迅速に決定し、優先順位スコアが最も高いインシデントに焦点を当てることができます。並べ替え、フィルタリング、担当者、およびステータスに関するさまざまなオプションをインシデントリストで直接変更できます。



インシデント対応

インシデントが作成されて優先順位付けが行われ、強化されると、侵害に迅速に対応することが重要になります。組み込みの対応ハンドブックにより、セキュリティアナリストとインシデント対応者がこれを実行できます。コンテキストハンドブックは、SANS の「PICERL」インシデント対応モデルに従う、段階的なガイド付きのインシデント対応を提供します。ハンドブック内のアクションの多くは、ネイティブの XDR 自動化ワークフローによって強化されます。これらのワークフローは、統合した製品に基づいてアクションを実行し、対応方法を決めるまでの時間を早めます。インシデントの作業ログでは、インシデントに関してすでに完了している作業の表示、重要な詳細が記載されたメモの投稿、チームとのコラボレーションが可能です。応答ハンドブックでの自動応答アクションの実行など、実行されたアクションの履歴を確認することもできます。すぐに使用できる、組み込みのワークフローを含む製品に依存しないハンドブックが利用可能です。これは、シスコが管理しています。一方、ハンドブックフレームワークは、さまざまなカスタマイズが可能です。ハンドブックは、複製して編集することも、最初から作成することもできます。[自動化（Automation）] のテンプレートを使用して、他のインシデント対応ワークフローを構築することもできます。また、このインシデント対応テンプレートでフィルタ処理することにより、Exchange でそれらを見つけることもできます。ハンドブック割り当てルールを使用すると、ユーザーはどのハンドブックをどのタイプのインシデントに割り当てるかを条件ロジックで定義できます。



脅威インテリジェンス

Cisco XDR プラットフォームでは、Cisco Talos やその他のソースからの組み込みの脅威インテリジェンスに加えて、脅威インテリジェンスの複数のソースを組み合わせることができます。これにより、インシデントの強化中、インシデントのさらなる調査と検証中、または脅威ハンティングの実行中に、重要なコンテキストが提供されます。この脅威インテリジェンスには、単純なレピュテーションから、攻撃ツール、手法、および既知の攻撃者間のより複雑な関係を含めることができます。ユーザーは、シスコとサードパーティの複数のインテリジェンス プロバイダーを有効にし、Cisco XDR Investigate 機能による調査で、ネイティブに統一してそれらすべてにアクセスできます。

脅威ハンティングと脅威調査

Cisco XDR Investigate 機能を使用すると、包括的でありながらシンプルなユーザーエクスペリエンスを提供しつつ、高度な脅威ハンティングを実行できます。調査中に、Cisco XDR はすべての統合をクエリし、ローカルとグローバルの両方の脅威インテリジェンスと、環境内の調査済み項目について報告された情報を取得します。その後、調査中のすべてのアーティファクトのグラフビューを、調整可能なタイムラインとともに表示できます。また、グラフフィルタとテーブルビューを使用して、特定の項目にすばやく焦点を当てることもできます。既存のインシデント、一連の監視対象に基づいて、またはテキストの一部（ブログの投稿など）をコピーして貼り付けることによって調査を開始します。Cisco XDR の豊富な API を使用すると、完全に自動化された調査を行うことも可能です。これにより、野放しになっている最近報告された一番の脅威を自動的に把握し、環境内で脅威の証拠が見つかった場合にプロアクティブにアラートを受け取ることができます。

サードパーティテレメトリ

Cisco XDR Advantage をご利用のお客様は、さまざまなベクトル、EDR、Email Threat Defense（ETD）、次世代ファイアウォール（NGFW）、ネットワークにおける検出と対応（NDR）、およびセキュリティ情報イベント管理（SIEM）で商業的にサポートされ、厳選された統合の利点を得られます。シスコがサポートし、厳選したサードパーティ統合のリストは動的に変更されるため、最新のリストについては、シスコの担当者にお問い合わせください。

統合

次に、Cisco XDR でサポートされている統合のリストを示します。シスコのオープンエコシステムでは、シスコのエンジニアリングだけでなく、開発パートナー、サードパーティ、さらにはユーザーも統合を作成できます。「C」が指定されている製品名は、シスコが作成したシスコが管理する統合です。「V」が指定されている製品名は、パートナーによって作成されたが、Cisco QA によって検証されたシスコ検証済みの統合です。どちらもサポート対象ですぐに使用できます。指定のない製品は、お客様によって Cisco XDR に統合されている場合があり、テストや検証が行われていない可能性があるソリューションです。このリストは、代表的なものであり、ここに記載されているソリューションが Cisco XDR と正常に統合されることを保証するものではなく、完全を意図したものではなく、いつでも予告なしに変更される可能性があります。各統合は、製品ベンダーと Cisco XDR がサポートできる製品機能とユースケースによって異なります。

アプリケーション、アイデンティティ、およびデバイス管理の統合

これらのソースには、デバイス、デバイスオブジェクト、またはユーザーの独自のインベントリがあり、この統合によって、これらのアセットに関する情報が Cisco XDR 内の一元的な場所に送られます。この包括的なビューによって、脆弱性の特定、脅威の防止、修復の優先順位付けをより適切に行うために必要なデータとコンテキストが提供されます。

- Cisco Duo[C]
- Cisco Identity Services Engine（ISE）[C]
- Cisco Orbital[C]
- Cisco Secure Access[C]
- Cisco Secure Web Appliance[C]
- Cisco Umbrella[C]

- Cisco Vulnerability Management（旧 Kenna）[C]
- Auth0[C]
- AWS[C]
- GitHub[C]
- Google Workspace[C]
- HRIS[C]
- Ivanti Neurons[C]
- Jamf Pro[C]
- Microsoft Entra ID[C]
- Microsoft Intune[C]
- Okta[C]
- Salesforce[C]
- Slack[C]
- VMWare Workspace ONE
- UEM[C]
- Workday[C]

コラボレーション、ITSM、チケット

コラボレーション、ITSM、およびチケットのツールにより、SOC チームはより効果的に連携して、アクションを追跡し、グループタスクを迅速に実行できます。Cisco XDR では、これらの統合により、タイムクリティカルまたはコンプライアンスのユースケースでこれらのツールを活用する自動化された手段を提供できます。

- Cisco Webex[C]
- Jira Cloud[C]
- Microsoft Teams[C]
- PagerDuty[C]
- ServiceNow[C]
- Slack[C]
- XMatters[C]
- ZenDesk

クラウドセキュリティの統合

クラウドセキュリティの統合は、セキュリティとコンプライアンスのリスクを軽減し、複数の製品にまたがるセキュリティポリシーを管理し、最もリスクが高い脆弱性と優先順位を下げることができる脆弱性を判断し、ハイブリッドワーク環境でアプリケーションを保護するのに役立ちます。これらの統合による追加の機能には、DDoS 脅威と OWASP 攻撃に対する保護、および Web セキュリティの拡張が含まれます。

- Cisco Defense Orchestrator[C]

- Cisco Secure Cloud DDoS Protection Service[V]
- Cisco Secure Cloud WAF Service[V]
- Cisco Secure Workload[C]
- Cisco Secure Web Appliance[C]
- Akamai
- Amazon Guard Duty
- **AppOmni（準備中）**
- Microsoft Graph Security API[C]
- Radware Cloud DDoS Protection[V]
- Radware Cloud WAF[V]
- Signal Sciences Next-Gen WAF

電子メールテレメトリと応答の統合

これらの統合により、脅威のコンテキストでメッセージ、送信者、およびターゲットの関係を可視化することで、脅威ベクトルとしての電子メールを把握できます。電子メール統合により、Control Center へのタイルとオーケストレーションのためのアクションが提供されるため、実務者は自動化されたワークフローを構築し、フィッシング攻撃、ビジネス電子メール詐欺、マルウェア、およびランサムウェアに対処するために、脅威のより優れたコンテキストを取得できます。

- Cisco Secure Email and Web Manager[C]
- Cisco Secure Email Gateway[C]
- Cisco Secure Email Threat Defense[C]
- Microsoft Defender for Office 365[C]
- Proofpoint Email Protection[C]

エンドポイント検出および応答テレメトリと応答の統合

EDR はすべての管理対象エンドポイントのリストを提供し、その詳細が抽出されて Cisco XDR の一元的な場所に保存されるため、信頼できない IP アドレスに依存することなく、デバイスが一意に識別され、アクションを実行できるようになります。エンドポイントコンテキストにより、SHA256 ハッシュに一致する複数のファイルとプロセス、およびこれらの主要なデータポイントが関連付けられている URL を調査して、有効性の高いインシデントに週次アラートを促進できます。これらは、攻撃による軽減、封じ込め、排除、または攻撃からの回復を行うための対応手順（ワンクリックまたは完全自動化）を取得するために不可欠です。

- Cisco Secure Client[C]
- Cisco Secure Endpoint[C]
- CrowdStrike Falcon Insight[C]
- Cybereason Endpoint Detection and Response[C]
- Microsoft Defender for Endpoint[C]
- Palo Alto Networks Cortex[C]

- SentinelOne Singularity[C]
- Trend Vision One[C]
- Qualys IOC

エンタープライズのバックアップ

バックアップ戦略は、効果的なセキュリティ対策の一部です。Cisco XDR では、バックアップテクノロジーとの統合により、予防および対応の両方のワークフローの一部として、手動および自動バックアップ、スナップショット、および復元アクションを推進できます。バックアップ テクノロジー パートナーとの統合が、Cisco XDR 自動ランサムウェアリカバリ機能の原動力になります。

- Cohesity Data Protect[V]
- Rubrik[V]
- PureStorage

ネットワークの検出と応答の統合

NDR は Cisco XDR のコアの基本的な統合です。エージェントレスの動作と異常の検出機能、および独自のネットワーク デバイス コンテキストによる脅威の検出を強化します。また、グローバル脅威インテリジェンスおよび内部可視性のソースと組み合わせて、既知の侵害インシデントに基づいて確認済みの脅威アラートを作成することができます。NDR は、インシデントの臨界を確認するために不可欠な、豊富なネットワーク デバイス コンテキスト セットも提供します。この履歴ネットワークデータは Cisco XDR によってクエリされ、脅威ハンティングとフォレンジックの監査と XDR インシデントを強化し、可視性を簡素化して、対応の効率を向上させます。

- Cisco Secure Network Analytics[C]
- Darktrace Respond & Detect[C]
- ExtraHop Reveal(x) 360[C]
- NETSCOUT Omnis Cyber Intelligence[V]
- Gigamon ThreatInsight

次世代ファイアウォールのテレメトリと応答の統合

NGFW デバイスの統合により、IP アドレス、URL、ドメインの検出情報を追加のコンテキストとして提供し、さらに Cisco XDR でのフォレンジック調査を実施できます。また、ユーザーは Secure Firepower を利用して、境界で IP をブロックできます。Cisco Secure Firewall デバイスは、トリアージされるアラートおよび関連付けられるアラートを Cisco XDR に提供するように設定し、Cisco XDR インシデントマネージャに最も影響度の高いアラートを表示することもできます。構成されたすべてのファイアウォールデバイスをクエリして XDR インシデントに関連する監視対象を強化することで、攻撃の可視性と理解度が向上します。自動応答機能と組み合わせて、それらを調整して使用するシングルクリック防御は、可視性を簡素化し、応答効率を向上させます。

- Cisco Secure Firewall[C]
- Cisco Meraki MX[C]
- Check Point Quantum Smart-1 Cloud[C]
- Cisco Adaptive Security Appliance[C]
- Fortinet FortiGate[C]
- Palo Alto Networks NGFW[C]
- Palo Alto Panorama[C]

パブリッククラウドの統合

Cisco XDR を主要なパブリック クラウド プロバイダーと統合して、フローログ、独自ログ、および API からネットワークメタデータを収集し、エンティティのモデリング、ベースライン、および悪意のあるネットワークアクティビティの検出のための強力なソースを提供します。エンティティモデリングでは、フローメタデータを使用して監視されたデバイスの動作から通常のアクティビティのモデルを構築し、このモデルを使用して、誤使用、マルウェア、または侵害が原因である可能性のある動作の変更を特定します。Cisco XDR では、クラウドプロバイダーを統合することで、セキュリティ オペレーション センター（SOC）が、署名をたどり続けながら、サイバー犯罪者や、終わりのない無数のエクスプロイト、マルウェア、その他の脅威の追跡を停止できるようにします。代わりに、SOC は、エンティティモデリングで識別された、確立されたパターンとアクティビティから、少数で優先順位が高く、自動的に検出された偏差にセキュリティの取り組みの焦点を当てることができます。

- Amazon Web Services（AWS）[C]
- Microsoft Azure[C]
- Google Cloud Platform（GCP）[C]

セキュリティ情報とイベント管理の統合

Cisco XDR は、クエリした脅威のアーティファクトとターゲットに関する監視およびレピュテーションのソースとして、脅威の調査中に SIEM を使用できます。サポートされている監視可能なタイプには、IPv4 アドレス、IPv6 アドレス、ドメイン、ファイル名、および SHA256 ファイルハッシュが含まれています。これらの統合により、調査者は Cisco XDR ワークフロー内のデータモデル間の変換レイヤとして統合を使用することにより、多くのデータソースから検出情報を収集できます。

- Cisco CESA[C]
- Cisco Splunk Cloud[C]
- Cisco Splunk enterprise[C]（準備中）
- Devo
- Google Chronicle
- Graylog
- Sumo Logic Cloud SIEM
- Sumo Logic Log Management

脅威インテリジェンスの統合

多数の脅威インテリジェンスソースへのアクセスが、追加コストなしで Cisco XDR に含まれています。これらには、Cisco Talos データベース、デフォルトのシスコ脅威インテリジェンス アーキテクチャ、ユーザーが独自の脅威インテリジェンスをアップロードできるプライベートリポジトリが、自社で生成したか他のソースから取得したかにかかわらず、含まれます。Cisco Secure Malware Analytics を Cisco XDR に統合することで、ユーザーはマルウェア、関連するネットワークトラフィック、システム変更などに関する詳細なインテリジェンスを取得し、さらにグローバルユーザーベースからの疑わしいファイルの自動デトネーションにより、マルウェアの脅威インテリジェンスを強化できます。

- Cisco Secure Malware Analytics[C]
- Cisco Talos Intelligence[C]
- Cisco Secure Endpoint File Reputation[C]
- AbuseIPDB IP Checker[C]
- AlienVault Open Threat Exchange[C]
- alphaMountain.ai Threat Intelligence
- Alspera CriminalIP
- APIVoid[C]
- Censys
- CyberCrime Tracker[C]
- Farsight Security DNSDB
- Google Safe Browsing[C]
- Have I Been Pwned[C]
- IBM X-Force Exchange[C]
- IsItPhishing
- MISP
- Palo Alto Networks AutoFocus
- Pulsedive[C]
- Recorded Future
- Red Sift Pulse[V]
- SecurityTrails
- Shodan[C]
- Sixgill Darkfeed
- SpyCloud Account Takeover Prevention
- Threatscore | Cyberprotect[C]
- urlscan.io[C]
- VirusTotal[C]

ライセンスオプション

Cisco XDR を利用できるライセンス階層は、Essentials、Advantage、Premier の 3 つです。

Cisco XDR Essentials は、いくつかの例外を除き、完全な XDR 機能を提供し、シスコのセキュリティポートフォリオ全体に統合します。**Cisco XDR Advantage** は、特定のサードパーティ製セキュリティツールとシスコが厳選した統合機能を追加することで、Essentials で提供される機能に構築されています。**Cisco XDR Premier** は、Advantage の全機能をシスコのセキュリティ専門家によって提供されるマネージドサービスとして提供します。これにはペネトレーションテストによるセキュリティ検証と特定の Cisco Talos Incident Response サービスが含まれています。

表 1. Cisco XDR ライセンスオプション

機能	Essentials	Advantage	Premier
セキュリティ分析と関連付け	✓	✓	✓
攻撃のインスタント検証付き攻撃ストーリーボード	✓	✓	✓
脅威インテリジェンス	✓	✓	✓
脅威ハンティング	✓	✓	✓
インシデント対応措置	✓	✓	✓
インシデントの優先順位付け	✓	✓	✓
ケースの優先順位付け	✓	✓	✓
アセットコンテキスト	✓	✓	✓
カスタム ワークフロー	✓	✓	✓
自動化ワークフローの交換	✓	✓	✓
データ取り込み/データ保持	✓	✓	✓
Cisco Software Support Enhanced	✓	✓	✓
シスコ アイデンティティ インテリジェンス	✓	✓	✓
サードパーティテレメトリ		✓	✓
Cisco Managed Extended Detection and Response			✓
Cisco Talos インシデント対応チーム（Talos IR）			✓
シスコ テクニカル セキュリティ アセスメント（CTSA）			✓

データ保持期間：デフォルトでは、90 日間のデータ保持期間が含まれます。お客様は、180 日間または 365 日間の追加の保持期間を購入することができます。

データ取り込み：各階層には、1 ユーザーに、1 ヵ月あたり 2GB のデータ取り込み制限があります。デフォルトの 2GB を超えた GB は、お客様が追加購入できます。これは、1 ユーザーに、1 ヵ月あたり GB 単位で測定されます。

Cisco Managed Extended Detection and Response

Cisco XDR Premier ライセンス階層は、シスコのセキュリティ専門家が提供する Cisco XDR ソリューションを使用する管理対象の検出および応答サービスです。ペネトレーションテストと特定の Cisco Talos インシデント対応リテーナーサービスによるセキュリティ検証が含まれています。Cisco XDR を利用した Cisco Managed Extended Detection and Response（MXDR）では、シスコの研究者、調査担当者、対応担当者のチーム、Cisco XDR ソリューション、統合ツールセット、および追加のシスコのセキュリティテクノロジー（利用可能な場合）を組み合わせて監視および対応し、潜在的なセキュリティ脅威や侵害に対処します。

Cisco MXDR サービスには次のものが含まれます。

- **24 時間 365 日のモニタリング：**専門のセキュリティ調査担当者によるグローバルなセキュリティインシデントとアラートのモニタリング。
- **シスコの比類のない専門知識：**シスコの研究者、調査担当者、および対応担当者チームは、Talos 脅威インテリジェンスと定義済み調査および対応ハンドブックの両方を活用して、脅威とアラートの検出、調査、および対応を支援します。シスコの回答には、脅威の種類や侵害の兆候に基づいて、追加情報、推奨事項、または変更が含まれる場合があります。
- **四半期ごとの脅威ブリーフィング：**Cisco MXDR インテリジェンスチームは、Cisco Talos Incident Response が共同で提供する、すべての MXDR のお客様を対象とするリモートレビュー会議を四半期ごとにホストします。この四半期ごとのブリーフィングでは、現在の脅威パターン、検出量、トレンドイベントに関する最新情報を提供します。
- **専用サービスポータル：**専用の Cisco MXDR サービスポータルでは、セキュリティインシデントのライフサイクル管理、ダッシュボードメトリック、ナレッジベース、SOC コミュニケーションなどが提供されます。
- **脅威アドバイザリ：**Cisco MXDR は、検出された新しい脅威に関する脅威アドバイザリを発行し、緩和制御の実装を通じてインシデントまたは侵害をプロアクティブに防止します。過去のすべてのインテリジェンス記事とアドバイザリは、Cisco XDR ポータルのナレッジベースを利用した MDR から入手できます。

Cisco Talos インシデント対応リテーナーサービス

Cisco Talos インシデント対応リテーナーサービスは、プロアクティブおよび緊急インシデント対応サービスのフルスイートを提供し、サイバーセキュリティ インシデントの準備、対応、およびリカバリを支援します。この柔軟なサービスを使用すると、次のようなメリットが得られます。

- **インシデント対応の専門知識：**経験豊富なインシデント対応者であるシスコのグローバルチームがアクティブなインシデント中に待機し、お客様の防御の強化を支援します。

- **迅速な対応：**アクティブなインシデントの報告から 4 時間以内に、インシデント対応担当者の 1 人をリモートで派遣することができます。これにより、ダウンタイムが最小限に抑えられ、インシデント解決が迅速化されます。
- **インテリジェンスで強化された分析：**脅威インテリジェンスのエバーグリーンライブラリを活用し、実証済みのインシデント対応プロセスを基盤としています。

シスコ テクニカル セキュリティ アセスメント

シスコ テクニカル セキュリティ アセスメントは、お客様のサイバーセキュリティ態勢を評価するためにプロアクティブなサービスのスイートを提供します。また、お客様が直面している脅威、脅威が実現する可能性、および実現した場合の運用レジリエンスへの影響に関するアドバイスも提供します。これには以下が含まれますが、これらに限定されません。

- 脅威のモデリング
- ペネトレーションテスト
- レッドチーム脅威シミュレーション
- セキュリティ アーキテクチャ アセスメント
- アプリケーション セキュリティ アセスメント
- セキュリティ運用アセスメント
- 開発運用セキュリティアセスメント
- デバイス設定とビルドのレビュー

サポート

Cisco XDR Software Support サービス

サポートには次の 2 つのレベルがあります。

- Cisco Software Support Enhanced は、すべての Cisco XDR ライセンス階層に追加料金なしで含まれています
- Cisco Software Support Premium は、追加料金で購入できます

Cisco Software Support Enhanced（同梱）

- ソリューションサポート（リアクティブなテクニカルサポート）：24 時間 365 日、30 分以内の応答時間のサービスレベル目標（SLO）
- 導入準備ガイダンス
- デジタル化の継続的な導入
- 定期的なセキュリティヘルスチェック：対象環境に対して年に 1 回

Cisco Software Support Premium（アドオン）

- Cisco Software Support Enhanced
- 指定されたカスタマーサクセス連絡窓口
- 導入セッションの拡張：1 年に最大 6 件の導入セッション
- 定期的なビジネスおよび成功のレビュー

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。

Printed in USA C78-4622850-01 05/25