

Cisco XDR でセキュリティ 運用を簡素化する

より多くを検出し、より迅速に行動し、
生産性を向上

目次

メリット	3
データに裏打ちされたインサイトによって包括的な脅威の検出と対応措置を実現	4
場所を問わず XDR を提供	5

Cisco XDR は、セキュリティチームによる検出と対応の方法を変えます。シスコのクラウドベースのソリューションは、セキュリティ運用を簡素化し、セキュリティチームが最も高度な脅威を検出、優先順位付けし、対応できるように設計されています。Cisco XDR は、シスコの幅広いセキュリティポートフォリオや選び抜かれたサードパーティ製品と統合された、今日の市場で最も包括的で柔軟なソリューションの 1 つです。

セキュリティ担当者によりセキュリティ担当者向けに設計された Cisco XDR は、アナリストは複数のソースからのデータを統合および関連付けして単一のビューにまとめることができます。これによって調査を合理化し、誤検知を減らし、アラートに優先順位を付け、検出から対応までの最短の経路を実現できます。

組み込みの自動化、オーケストレーション、ガイド付きの修復方法の推奨により、アナリストは反復的なタスクを自動化し、脅威をより効果的に軽減し、時間とリソースを解放して他の重要なセキュリティタスクに集中できます。

データ主導の Cisco XDR アプローチにより、SOC チームは最も影響の大きいイベントを定義し、修復戦略の焦点をそのイベントに当てることができます。これによって組織の全体的なセキュリティ体制を強化し、回復力を向上できます。

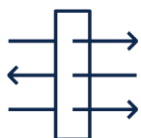
メリット



ベンダーやベクトルに関係なく可視性を統一し、盲点を回避

ネットワーク、クラウド、エンドポイント、Eメール、アプリケーション全体で可視性を確保し、脅威を特定して、マルチベンダー、マルチベクトル環境全体で効果的なセキュリティを実現します。

Cisco XDR は、複数の異なる検出テクノロジーからのデータを統一ビューに関連付けることにより、より迅速で簡素化された調査を可能にし、対応を合理化します。



脅威の検出と対応を加速し、真に重要なことに対処

複数のテレメトリソース間で検出を関連付けて、最大のリスクがある脅威を優先します。

AI と機械学習を活用することで、Cisco XDR は精度の高い相関検出を可能にし、不要な情報を減らし、セキュリティのリスクとビジネスのリスクを効果的に調整します。



証拠に裏打ちされた推奨事項によって対応を自動化し、影響を最小化

自動化とガイド付きの推奨対応方法を使用して、関連するすべてのコントロールポイントにわたって自信を持って脅威を修復できます。

調査時間を短縮し、対応を加速することで、Cisco XDR は SOC チームの対応力を引き上げ、回復力を強化します。

データに裏打ちされたインサイトによって包括的な脅威の検出と対応措置を実現

複雑な脅威をより迅速に検出

- **Cisco XDR** は、エンドポイント、Eメール、ネットワーク、クラウド、ファイアウォールなどにわたる幅広い組み込みの統合と、最も柔軟で、スケーラブルで、効果的な **XDR** 戦略のための厳選されたサードパーティの統合を実現します。
- オンプレミスネットワークとパブリッククラウドおよびプライベートクラウドからのテレメトリを活用して、管理対象デバイスと管理対象外デバイス上の脅威を検出し、イベントを関連付ける際に重要なコンテキスト（攻撃の開始場所やネットワークでの広がり方など）を取得します。
- **Talos** の脅威インテリジェンスは検出機能を強化するため、アナリストは他に類を見ない実用的な情報を収集し、現実世界の脅威の動作に関するコンテキストをより深く把握することによって、既知の脅威と新しい脅威を明らかにできます。

影響によって脅威に優先順位を付け、最も重要なことに迅速に対処

- リスクベースの優先順位付けにより、**SOC** アナリストは最大の脅威となるアラートに集中できるため、迅速かつ効果的なアクションを実行できます。この独自のアプローチにより、実際の重大度に応じてアラートに優先順位が付けられ、単一のビューで確認できます。
- 特定、封じ込め、根絶、復旧を支援するガイド付きの対応により平均対応時間（**MTTR**）を短縮します。組み込みの対応措置と組み合わせることで、一貫した効果的な意思決定に役立ちます。
- 統一されたコンテキストとプログレッシブ開示の手法により、調査時間を簡素化および短縮します。**Cisco XDR** は、アナリストに必要な情報を提示します。分析の停滞につながる無関係なデータを大量に提供することはありません。必要に応じて、詳細に調査するための情報をクリックするだけでいつでも入手できます。

対応の迅速化

- 組み込みの対応措置とオーケストレーションにより、脅威を迅速に修復します。**Cisco XDR** を使用することで、**SOC** チームは事前に構築され、カスタマイズも可能なさまざまなオーケストレーションワークブックを活用して、わずか数クリックで脅威をシャットダウンし、リスクを軽減できます。
- 反復的で時間のかかるタスクを自動化し、**SOC** チームにすぐに使用できるベストプラクティスを提供することで、限られたリソースを最大限に活用して価値を最大化できます。自動化が適切でない場合、**Cisco XDR** は、**SOC** アナリストが効果的な対応措置を実行できるように、ガイド付きの対応提案と推奨事項を提供します。
- 組み込みのシスコソリューションとサードパーティ両方のさまざまなセキュリティコントロールポイントに緊密に統合されているため、幅広いセキュリティツールにわたって対応措置を迅速にプッシュできます。異なるアラートログを調査することで脅威ハンティングにおいて先手を打つとともに、侵害の新しい戦略、テクニック、兆候を学ぶことができます。

場所を問わず XDR を提供



あらゆるビジネスに対応する柔軟なオプション

Cisco XDR には、次の 3 つのライセンス階層があります。

- **Cisco XDR Essentials** はすべての 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を統合します。
- **Cisco XDR Advantage** は Essentials の機能に加えて、シスコが厳選したサードパーティ セキュリティ ツールとの統合機能が組み込まれています。
- **Cisco XDR Premier** では、Advantage のすべての機能がマネージドサービスとしてシスコのセキュリティエキスパートにより提供されます。その他にもペネトレーションテストによるセキュリティの検証、Cisco Talos インシデント対応サービス、シスコ テクニカル セキュリティ アセスメント サービスを利用できます。

Cisco XDR の詳細についてはこちら：cisco.com/go/xdr

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。

[製品に関して](#) | [サービスに関して](#) | [各種キャンペーンに関して](#) | [お見積依頼](#) | [一般的なご質問](#)

お問い合わせ先

お電話での問い合わせ

平日 9:00 - 17:00

0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback



©2023 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systems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一定の国における商標登録または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は2023年9月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

cisco.com/jp