XDR バイヤーズガイド

新しい Extended Detection and Response 市場の製品のスムーズな選定に役立つガイド

© 2022 Cisco and/or its affiliates. All rights reserved.

目次

Extended Detection and Response（XDR）について 3

XDR を検討する主な理由： 3

適切な XDR に必要な 5 つの要素 5

XDR の導入に向けて 7

XDR + セキュリティレジリエンス 7

XDR ベンダー評価ワークシート 8

詳細 9

© 2022 Cisco and/or its affiliates. All rights reserved.

Extended Detection and Response（XDR）について

新しいセキュリティアプローチが必要とされている理由

潤沢な資金がある優れたセキュリティチームでさえも、外部からの大きな圧力を自覚しています。昨今進んだリモートワークやハイブリッドワークへの移行も、この事態を更に複雑なものにしています。攻撃対象領域は絶えず拡大しています。無限に発生するアラート。互換性に乏しいセキュリティツール。人とテクノロジーが良好な関係を築けなければ、セキュリティ対策の有効性は十分に発揮されません。およそ 280 日と言われる平均滞留時間に改善が見られないのもそのためです[1]。

こうした新しい日常に、セキュリティレジリエンスが求められています。セキュリティレジリエンスとは、ビジネスが先例のない脅威や変化に耐え、かつ一層の強靭性をもって回復できるよう、あらゆる側面でビジネスのインテグリティを守ることです。今、セキュリティレジリエンスには、これまで以上の対策が求められています。

XDR を検討する主な理由：

- アラート疲れの軽減
- 検出時間の短縮
- ツール全体での可視性の向上
- 脅威のコンテキストの一層明確な把握

[1] IBM の『2020 年データ侵害のコストに関する調査レポート』で紹介された、Ponemon Institute による調査

© 2022 Cisco and/or its affiliates. All rights reserved.

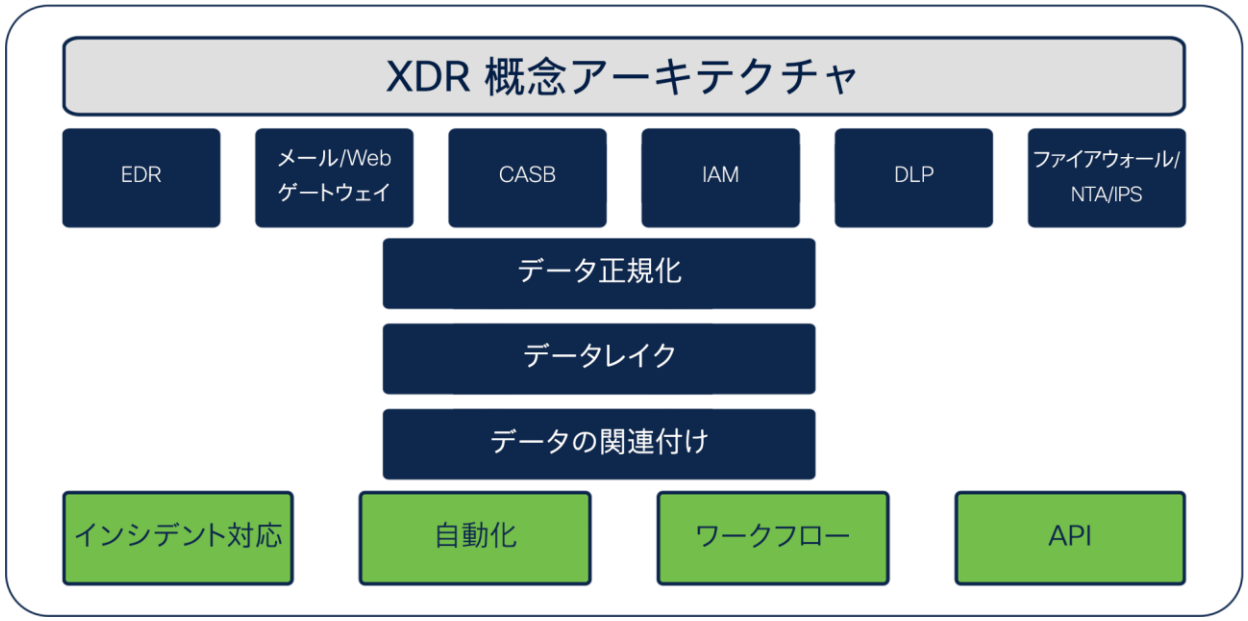
XDR とは何か？重視すべき理由は？

セキュリティチームにとって、セキュリティ ポイント ソリューションをネイティブに統合した DXR は非常に有益である一方で、組織にとっても、既存のサードパーティテクノロジーと容易に接続し活用できるプラットフォームは、ROI を向上させ、すべてのデータソースにより豊富なコンテキストを提供できる観点から非常に重要です。XDR は、大半の検出/対応を個々の製品サイロやチーム内で実施している現在の戦略からの大きなパラダイムシフトと言えます。XDR が実現する統合は、どのセキュリティチームにも関わる複数の重要な領域に効果をもたらします。

第 1 に XDR は、ほとんど調整を必要とせず、チームに迅速に価値を提供します。チームが SIEM や SOAR を設定済みの場合、これらの機能を基盤に XDR を構築できます。

第 2 に、非常に多くのチームに広まっているアラート疲れを解消します。このプラットフォームは、同じ侵害によって引き起こされたすべての異なるイベントを集約してインシデントに関連付けます。

第 3 に、すぐに利用できる自動化およびオーケストレーション機能を活用して、日常的な定型業務をなくすことができます。



© 2022 Cisco and/or its affiliates. All rights reserved.

適切な XDR に必要な 5 つの要素

1. どの環境からも収集できる包括的なテレメトリ

XDR に欠かせない基本的な機能は、幅広い可視性と深いインサイトです。現時点では、多くのベンダーは既存の自社製品を XDR の重要なコンポーネントとして位置づけています。しかし、真の XDR はただデータを結びつけるだけでなく、複数のセキュリティコントロール、データレポジトリ、脅威インテリジェンスベンダーなど幅広い層からのテレメトリをも収集し、悪意のあるアクティビティを検出します。オープンで統合された XDR プラットフォームを導入することで、企業や組織は、キャンパス、データセンター、クラウド、クラウドエッジなどのエコシステムに残る隙間を埋め、全体をくまなく防御できます。XDR に統合されたソリューションから抽出される有益なコンテキストによって、早期に脆弱性を検出し修復できます。

主な機能	質問事項
環境全体のインサイト	ご提案のソリューションには、ネットワークの可視性以外に、当社にとってどのようなメリットがありますか？
実用的なテレメトリ	インサイトや重要なテレメトリの提供のためにデータレイクを使用していますか？
信頼できるデータソース	ご提案のソリューションは、どのようにしてネットワークに出入りするすべてのエンドポイント、デバイス、トラフィックに関するコンテキストをユーザーに確実に提供するのですか？

2. ベンダーにかかわらず、既存の投資の検出機能を活用

ガートナーは XDR の定義に独自仕様のコンポーネントという言葉を使っていますが、XDR ソリューションが、サードパーティテクノロジーと簡単に接続できるオープンプラットフォームで構築されることは重要なポイントです。セキュリティスタックの各コンポーネントには、IoC 検出、機械学習、行動分析など、それぞれに特有の検出機能を持っており、それらを統合するとさらに高精度な検出が実現します。サイロではわずかな兆候でも、統合することでより明確に捉えることができます。XDR の有効性を最大限に活かすには、すべての検出機能がシームレスに連携することが大前提です。セキュリティスタック全体で機能するプラットフォームを選びましょう。

主な機能	質問事項
既存のソリューションを活用	ご提案の XDR アプローチでは、当社の既存の投資をどれくらい活用できますか？
ベンダーに依存しない	ご提案の検出テクノロジーは、市場の他のテクノロジーとどのような違いがありますか？
サードパーティの分析を取得	すぐに相互に統合できるのはどのソリューションですか？

© 2022 Cisco and/or its affiliates. All rights reserved.

3. 信頼できる情報源のコンテキストを統合し、迅速で正確な対応をサポート

ネットワーク、エンドポイント、メール（およびその他の多くの要素）から得られたインサイトが統合されると、発生している事象、その進行状況、脅威の修復に必要な手順について、より正確に理解できます。効果的な XDR は、ホストの隔離や、すべての受信トレイからの悪意のある電子メールの削除など、ネイティブな対応および修復機能を備えています。理想的には、これらのアクションは 1 ～ 2 回のクリックで実行できます。時間の経過とともにチームがセキュリティを進化させることができるように、XDR にはカスタム対応措置を容易に作成できる機能も必要です。

主な機能	質問事項
コンテキスト主導のインテリジェンス	ご提案の XDR を使用すると、脅威の影響や侵害の範囲を理解し、単一のインターフェイスから 1 回のクリックで措置を講じられますか？
複数の信頼できる情報源	ご提案の検出機能を提供するのはどのようなタイプの脅威インテリジェンスですか？そのインテリジェンスの提供元はどこですか？
MTTD の向上	ご提案のソリューションで使用するデータソースをどのように検証していますか？

4. マシンスケールの問題の解決のために継続的に自動化とオーケストレーションを提供

煩雑な手作業や旧式のワークフローは、企業や組織をさまざまな脅威やヒューマンエラーにさらします。適切な XDR プラットフォームは、強力なオーケストレーションと自動化機能を備えており、反復的なセキュリティタスクを楽に、効率的に実行します。システムの習得に多くの時間はかかりません。重要なワークフローを自動化することで、チームはアラートに迅速に対応できるようになり、その結果、脅威ハンティングなどの重要なタスクにより多くの時間と労力を費やせるようになります。

主な機能	質問事項
自動化の強化	サードパーティとの統合で、ベンダーが API を変更した場合に自動化スクリプトに影響は出ませんか？
セキュリティノイズの見極め	既存のソリューション全体のワークフローのオーケストレーションと自動化を支援できますか？
人的な限界の克服	ご提案のソリューションは、クラウドベースのワークロードとの間の監視をどのようにサポートできますか？

© 2022 Cisco and/or its affiliates. All rights reserved.

5. 1 ヵ所で調査を実施し、容易な隔離と修復を実現

XDR は、セキュリティチームのツールキットを拡充し、エンドポイントだけにとどまらない豊富なテレメトリを可視化します。1 つのコンソールで、直接修復や脅威インテリジェンスへのアクセスができるほか、アラートを 1 つの画面で管理できるツールも備わっています。また、XDR は脅威ハンティングに MITRE ATT&CK などの仕組みを用いているため、経験の浅いメンバーでも仮説主導型の脅威ハンティングが実行でき、次に何が起こるかを把握し備えられます。

主な機能	質問事項
MTTR の向上	ご提案のソリューションは、どのような修復を支援/加速しますか？
脅威ハンティングの拡大	ご提案のソリューションは、当社のチームの脅威ハンティングをどのように支援できますか？

XDR の導入に向けて

私たちは、お客様にとって最適な XDR 戦略を決定するため、XDR の関係者と協力することをお勧めしています。潜在的なベンダーが自動化と統合を優先していることを確認します。

目に見える成果を達成し、高い ROI をもたらすために、現在お使いのスタックの機能や条件をよく理解した上で、以下の質問にお答えください。

1. ご提案の XDR 製品は、ネットワークの検出と対応、および電子メール、クラウド、ファイアウォールなどの他のセキュリティレイヤーをカバーしていますか？
2. 情報に基づいたより適切なセキュリティ措置の実行をどのようにして支援できますか？
3. ご提案の XDR はブロックや修復の自動化にどのように役立ちますか？
4. 設定変更を必要とせずに他のツールと統合できるソリューションはどれですか？
5. ご提案の XDR ソリューションは、SASE やゼロトラストなどの他のセキュリティ対策とどのように結び付いていますか？

XDR + セキュリティレジリエンス

今は運用から財務、サプライチェーンに至るまで、不確実性を伴う時代です。企業や組織は、不測の事態を受容し、かつ一層の強靭性をもって適応できるレジリエンスの強化に投資を拡大しています。しかし、その努力もセキュリティレジリエンスへの投資なしでは意味をなしません。

セキュリティレジリエンスの 5 つの特徴

1. エコシステム全体で何十億ものシグナルを活用。
2. インテリジェンスを共有して、次に起こることを予測。
3. リスクベースでコンテキストを分析し、アラートの重要度を決定。
4. ソリューションを統合し、エコシステム全体でのギャップを解消。
5. オーケストレーションと自動化によってシステムを強化。

適切な XDR プラットフォームは、これらの特徴を備えています。ユニファイドコンテキスト、相関性のある検出機能、迅速な対応能力。これらを備え、XDR の可能性を引き出せるのはシスコだけです。

© 2022 Cisco and/or its affiliates. All rights reserved.

シスコの全セキュリティ製品に付属する SecureX は、オープン API を活用しお使いの環境のセキュリティソリューションに簡単に統合できるセキュリティ プラットフォームです。統合された検出と応答レイヤーは、全てのコントロールポイントからのテレメトリを関連付け、単一の視点で可視化するため、優先順位の決定と実行が容易になります。また、組み込まれたオーケストレーション機能により、応答を自動化し、ルーチンタスクをオフロードすることで、チームメンバーは脅威ハンティングなどのより積極的なタスクに集中することができます。

もう迷う必要はありません。ぜひ導入をご検討ください。

XDR ベンダー評価ワークシート

XDR ベンダーとの会話に、こちらの表と、以前ご紹介した質問集をご活用ください。お客様の環境に最も重要な 8 ～ 10 の質問を選択し、コピーして以下に貼り付けてください。

質問/メモ	魅力的な回答
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	
質問：	
メモ：	

© 2022 Cisco and/or its affiliates. All rights reserved.

詳細

シスコの XDR ソリューションについてさらに詳しくお知りになりたい方は、シスコ営業担当者にお気軽にお問合せください。

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

©2022 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2022年11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

1128-2022-000-X