Secureworks® | Taegis™ XDR

ご購入ガイド

Extended Detection and Response (XDR)

はじめに

Extended Detection and Response (XDR) は、サイバーセキュリティ業界を席巻する新たな概念と目されています。リサーチおよびアドバイザリーサービスを提供するガートナー社は、XDR を 2020 年の “Security and Risk Trend” (「セキュリティおよびリスクに関するトレンド」) の第一位に、そして 2021 年の “Security and Risk Trend” in 2020[1]” (「セキュリティプロジェクト」のトップ 10) に挙げました。また、数々の業界ブログで「セキュリティの次なる進化」として XDR が取り上げられています。XDR がバズワード的な盛り上がりを見せるなか、IT およびセキュリティ部門のリーダーらは、脅威検知・対応のあり方を変革する XDR の潜在的な影響力をいち早く認識しはじめています。

高度な脅威検知に対する大きなニーズ

IT 専門家の 83%が、脅威検知・対応ソリューションへの予算を拡大しています[2]。

XDR ソリューションは現在、成熟サイクルの初期段階ではありますが、お客様の関心は急速に高まっています。検知・インシデント対応機能が集約されている XDR を活用することで、ポイントソリューションや SIEM のレガシーシステムでは通常見過ごされるような複雑な攻撃も特定できます。

XDR ソリューションについて

XDR は元々、「セキュリティオペレーションの簡素化と高度な脅威検知」を求めるお客様のニーズによって誕生しました。悪意ある第三者やその活動に対する効果的な特定手段を模索する組織にとって、「新たな脅威をいち早く検知すること」は必須条件となっています。

XDR の主な機能

42%

Visualization of complex attacks[2]

複雑な攻撃の可視化率[2]

38%

Analytics to detect modern attacks[2]

分析機能によるモダンアタック (最先端の攻撃) 検知率[2]

31%

Improved mean time to detect (MTTD)[2]

検知までの所要時間 (MTTD) の短縮[2]

[1] Gartner, Smarter with Gartner, 2020
[2] ESG, The Impact of the Modern SOC, 2020

セキュリティオペレーションに問題を抱える組織にとって、効率性と生産性の改善および自動化が保証されていることも、XDRの大きな魅力のひとつです。

競争が激しいXDRの市場では、セキュリティソリューションプロバイダーがこぞって自社製品をアピールしています。こうした状況で、ITおよびセキュリティ部門のリーダーらは一時的な盛り上がりに踊らされることなく、適切なXDRベンダーを見極めなければなりません。本ガイドでは、「XDR製品への投資を決断する前に確認すべき質問」を15項目ご紹介します。

脅威動向の把握

業務変革によって人々の働き方や就業場所が大きく変化するなか、脅威を取り巻く動向も刻々と進化しています。何百万人もの従業員が本社などのオフィスではなく自宅をはじめとするリモート環境で勤務するようになり、攻撃対象領域が大幅に拡大しました。サイバー犯罪者はこの環境に素早く適応し、個人宅ネットワークへの攻撃件数も急増しています。

さらに、悪意をもった第三者は、検知されにくい複雑な攻撃を仕掛けてきます。Ponemon Instituteが最近実施した調査では、こうした高度な攻撃による影響を次のように解説しています。

- An average of 80% of successful breaches are new or unknown "zero-day attacks"[3]
  侵害事案の平均80%は、新種の攻撃または未知の「ゼロデイ攻撃」[3]
- Zero-day attacks are expected to more than double in the coming year[3]
  ゼロデイ攻撃は今後1年間で2倍以上に増える見込み[3]

この新たな現実を見据えた脅威動向への適応準備ができていない組織は、今後数年間にわたり残念な結果に苦しむ可能性があります。

セキュリティツールの連携

事後対応的なセキュリティ対策では、今日の新たな脅威や標的型攻撃から組織を効果的に保護できません。組織のインフラ保護策として実装される多数の縦割り型セキュリティツールを管理するために時間や工数を取られるセキュリティチームは、攻撃者に後れを取ってしまいがちです。ソリューション同士が充分連携されていないため、セキュリティアナリストは散在するデータを手動でつなぎ合わせる作業や、分離独立する製品の管理やトラブルシューティングの作業に時間を取られ、「真の脅威」の追跡調査がおろそかになってしまいます。さらに、セキュリティオペレーションチームの人員不足やスキル不足という問題も克服しなければなりません。

SIEMのレガシーシステムやポイントソリューションにはこうしたオペレーション面での不備に加え、水面下で進行する非常に巧妙な脅威を特定する機能が足りない、という特性があります。統合型のインシデント検知・対応ソリューションが導入されていない多くの組織は、セキュリティ態勢が不十分な状態で、ビジネス情勢の変化に後れを取るまいと悪戦苦闘しています。

SecOpsの有効性を高めるXDR

58%

of IT pros believe XDR could improve the capabilities of security analysts.[2]

IT専門家の58%は、「XDRを活用することでセキュリティアナリストの能力を強化できる」と考えています。[2]

[3] Ponemon Institute, The Third Annual Study on the State of Endpoint Security Risk, 2020

XDR：新たな現実に対する新たなアプローチ

XDRは脅威検知・対応の進化形ソリューションであり、EDRが取りこぼした情報を捕捉し、検知・対応機能をエンドポイント以外のネットワークやクラウド環境にまで拡張する、という基本特性を備えています。前述のガートナー社は、XDRを次のように定義しています。

XDR "describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components."[4]

XDRとは「個々の組織で使用される複数のセキュリティコンポーネントからデータを自動的に収集して関連付ける、統合されたセキュリティインシデント検知・対応プラットフォーム」を指します。[4]

「SOCツールのアーキテクチャ構成時の優先課題」についてたずねられたIT専門家の90%以上が、「ツール同士の連携」をトップ5のひとつに挙げており、37%が当該項目（ツール同士の連携）を最重要課題として挙げています[2]。縦割り製品の防御・検知・対応機能を統合することで、脅威の可視性が向上し、通常であればポイントソリューションをすり抜けるようなステルス性の脅威も特定できます。検知機能一体型ソリューションの内部で最初に実行される処理は、過去およびリアルタイムのイベントデータを共通データフォーマットに変換し、一元リポジトリに格納すること（システム処理のための体系化）です。脅威アクティビティの全体像をもとに、XDRが収集・監視データや脅威インテリジェンスのデータの相関付けを行い、それぞれの関係性および悪意が疑われるトレンドを特定します。コンテキスト情報が補完された高精度のデータをもとに検知・対応をスピードアップできるため、セキュリティチームの業務にも役立ちます。

アラートノイズから真のアラートを選別し、新たに押し寄せる攻撃の波に合わせた対応が求められるセキュリティオペレーションの業務はかつてないほど困難になっています。散在するポイントソリューションの運用にはそれぞれ異なる管理手法と専門知識が必要です。こうした複雑性が、セキュリティチームの生産性を大きく損ねています。複数のセキュリティコンポーネントを一元的な検知・対応ソリューションに統合したXDRを活用することで「回転イス式の管理」から脱却し、アナリストの作業効率を高めることができると共に、経験の浅いアナリストの能力も底上げできます。XDRはオペレーションの生産性向上と脅威検知機能の強化を通じて、業務変革を支援します。

XDRベンダーの選定における重要な評価基準

セキュリティの有効性とオペレーション効率の改善

理想的なXDRソリューションの条件は、防御・検知・インシデント対応機能が一元化され、未知の高度な脅威に対処できること、およびオペレーションの生産性を改善できることです。さらに、セキュリティチームのアラート疲れを解消し、より重要な脅威に時間を振り向けられるよう、相関付けやアラート検証の自動実行機能を搭載していることも必須条件です。

脅威に対する防御効果をより詳しく理解するには、ベンダーが「攻撃者のアクティビティに関するインテリジェンスをXDRに反映し、ソリューションを常に最新の状態に保っているかどうか」を見極める必要があります。

[4] Gartner, Innovation Insight for Extended Detection and Response, 2020

Secureworks®

選定候補のベンダーに確認すべき５つの質問

- 検討対象のソリューションで検知可能な脅威や悪質アクティビティの種類
- 脅威インテリジェンスのソース（どのような情報源にもとづくインテリジェンスなのか）
- MITRE ATT&CK フレームワークにもとづくアラート項目マッピングの有無
- ランサムウェアなどの攻撃が実害に発展する前に、どの程度効果的に阻止できるか？
- 異常検知や侵害指標の特定に用いるテクノロジーの種類

オープンアーキテクチャ

XDR ソリューションは主に、クローズド型（専有型）とオープン型の２種類があります。前者は、ベンダーが自社のセキュリティソリューション製品群を一元的 XDR 管理プラットフォーム上で統合する形態であり、お客様側で導入済のセキュリティ対策システムを「総入れ替え」する必要があります。さらに、ベンダーの製品ポートフォリオでカバーできないサービスがある場合、有効性が薄れてしまう恐れがあります。

オープン型の XDR は、単一ベンダーのソリューションとは対照的に、最適なセキュリティ製品を選定して組み合わせ、一元的に管理・分析を統合します。XDR ベンダーを検討する際は、ご利用中のセキュリティツールとの「互換性」および、将来的に外部製品を追加することになった場合の「柔軟性」も必ず確認しましょう。

データの集約・保管コスト

IT 専門家の 40％が、「データの取得プロセスを改善してリアルタイムのデータソースにも対応できれば、セキュリティの有効性と効率が改善する」と考えています[2]。デジタルトランスフォーメーションの加速に伴い、何テラバイトものリアルタイム／バッチデータを一元化し、相関付け・分析するための性能が XDR に求められます。縦割り型のセキュリティシステムでは死角が生まれ、全社的なエコシステムで可視化されないままデータが放置されてしまいます。XDR の重要な役割は、データを一元的なリポジトリ上に集約・正規化し、分析で使える状態にすることです[5]。

クラウドネイティブプラットフォーム上に XDR ソリューションを構築するベンダーは、異種ベンダーの製品が収集するデータを容易に統合できると同時に、業務ニーズに合わせたデータ量の増加に対処可能な拡張性も提供します。

データの取得・保管コストも検討すべき課題です。「データ維持コストが高すぎるため、重要かもしれないデータのいずれかを消去しなければならない」というのは本末転倒です。ベンダー選定時にはこの点も考慮しましょう。

確認すべき6つの質問

- インフラの改修や新たなテクノロジーの実装が必要になるか？ベンダーのテクノロジースタックに合わせて現行システムを作り替える必要があるか？
- ソリューションのカバー対象環境（例：クラウド／エンドポイント／ネットワーク／すべて）および対応形態（個別にカバーするのか、すべてを一体的にカバーするのか）
- 既存のセキュリティシステムが収集するデータを一元化して分析できるか？
- ログ情報として収集・維持する情報ソースの種類は？ログ情報を直接検索することは可能か？
- 取得対象となる膨大なデータの収集・格納・処理・分析方法
- データの取得・保管コスト、およびデータの保管期間

既知および未知の脅威の防御・検知・対応

複雑な脅威環境で自社を守ろうとする多くの組織にとって通常、最初の防衛線はエンドポイントです。無数の攻撃を阻止するには、既知および未知の脅威をエンドポイントで自動防御すると同時に、調査の負担を軽減し、侵入防止段階で得られたデータをXDRの一要素として反映できる機能が不可欠です。機械学習ベースの次世代侵入防止（NGAV）ソリューションは、エンドポイントのパフォーマンスへの影響を最小限に抑えながら、新種の高度な脅威を検知します。さらに、機械学習モデルをローカル搭載した侵入防止ソリューションは、オフライン状態であってもエンドポイントを確実に保護できるため、シグネチャを頻繁に更新する必要はありません。効果的な防御機能を搭載したXDRを活用することで、セキュリティチームはエンドポイント対策をすり抜けて侵入する攻撃に集中できます。防御・検知・対応機能をXDR上に統合することで、脅威の検知および調査プロセスを改善し、スピードアップします。

確認すべき6つの質問

- 防御・検知・対応機能がソリューションに一体化されているか？
- 侵入防止システム／NGAVのデータをソリューションに取り込んで分析できるか？
- XDRコンソール経由でエンドポイントの修復措置を実行できるか？
- XDRの侵入防止機能を使って高度な脅威（ゼロデイ攻撃や変異型マルウェアなど）をエンドポイントで自動ブロックできるか？
- XDRの侵入防止機能／NGAVを稼働させると、エンドユーザーの端末にどの程度の影響が生じるか？
- デバイスがオフライン状態でもエンドポイントを確実に保護できるか？

Secureworks Taegis™ XDRで先手を打って攻撃者に対抗

サイバー攻撃の巧妙化、ステルス化に伴い、多くの企業や政府機関は後れを取るまいと悪戦苦闘しています。ハイブリッド型IT環境の死角、セキュリティチームの人員不足、散在するセキュリティツールの管理コストや複雑性の増大などの問題を抱える組織には、既存のセキュリティインフラを統合可能な「Extended Detection and Response (XDR) ソリューション」が必要です。なかでも、実用的で的確な知見を導き出すと共に、単一コンソール上で高度なオートメーション機能を駆使して脅威を調査し、迅速に対応可能なソリューションが強く求められています。

20年以上にわたって業界をリードしてきたセキュアワークスの原動力であるセキュリティオペレーションのノウハウや脅威動向に関する豊富なナレッジが集約されたクラウドネイティブ型のSaaSプラットフォーム「Taegis XDR」が、皆様のセキュリティオペレーションの効果・効率を高めます。

- お客様組織のセキュリティファブリック全体で収集した監視データを集約し、エンドポイント、ネットワーク、クラウド環境すべてを可視化してコントロール
- AIを駆使した分析および、セキュアワークスのカウンター・スレット・ユニット™が生成した包括的な脅威インテリジェンスで高度な脅威を検知
- あらゆるデータ、脅威ハンティングツール、自動対応プレイブックが集約された使い勝手の良いクラウド型コンソールの単一画面で、調査とインシデント対応をスピードアップ

防御・検知・対応機能の統合

受賞歴のあるTaegis XDRの検知・対応機能と、Taegis NGAVの次世代エンドポイント侵入防止機能が一体化された直感的かつ包括的な防御・検知・対応ソリューションです。

脅威をより迅速かつ正確に検知

エンドポイントから侵入する脅威をTaegis NGAVが自動で阻止します。また、セキュアワークスのカウンター・スレット・ユニット™が生成する脅威指標、対抗策、個別分析項目をもとに常時更新されるTaegis XDRの高度な分析エンジンがお客様環境の至る所で高度な攻撃を検知します。実証済みかつ優先度分類済のアラートをもとに「真の脅威」をいち早く特定できるため、誤検知対応に追われずに済みます。

セキュリティオペレーションのモダナイズ

Taegis XDR上でセキュリティインフラ全体を可視化し、あらゆる調査を一元的に実施できるため、手作業でデータをつなぎ合わせたり複数のツールを使い分ける必要はありません。年間1,400件を超える当社のインシデント対応案件のノウハウが反映された対応アクションのレコメンデーションおよび自動対応プレイブックを活用することで、平均修復時間 (MTTR) を数分単位に短縮できます。

Taegis XDRについて：
お客様や外部リサーチ会社アナリストから寄せられたコメント

「XDRには、セキュリティ分析機能と高度な補完的ツールがこれまでにない形で融合されおり、我々が見過ごしていたような脅威も逃さず検知します。単なる次世代SIEMではなく、新たな進化形ソリューションです」

Ricoh USA, Inc.
コーポレート・情報セキュリティ部門VP兼CISO
David Levine氏

「セキュリティ関連のイベントを迅速に特定して対応することが我々にとって最大の課題でした。Taegisの稼働をスタートした当日の夜に早速、疑わしい活動に関するアラートや、具体的かつ実用的な推奨策が届きました。これほど早くアラートを入手できたのは初めてです。これで、チームのセキュリティ態勢強化に向けて大きな一歩を踏み出せました」

GKN Wheels and Structures社
グローバルITディレクター
Faisal Jaffri Global博士

「Taegis XDRは、ベンダーであるセキュアワークス自体が長年使っている実証済みツールをベースとした各種セキュリティ対策システムが収集する監視データの分析、相関付け、可視化だけでなく、同社の脅威検知・対応専門チームが生成する充実した脅威インテリジェンスおよび実証済みの攻撃対抗策も提供します」

ESG社
上級セキュリティアナリスト
David Gruber氏

「Taegis NGAVは成熟した製品であり、小規模な環境から多国籍企業まで様々な導入形態に対応できます」

「安定した性能で、実際に出回っているマルウェアを確実に検知し、すぐにSOCに実装可能なコンソールやフィーチャー群を備えたSecureworks Taegis NGAVがITセキュリティ対策のラインアップに加われば心強いでしょう」

MRG Effitas社が2021年8月に公表した有効性評価レポート
「Efficacy Assessment of Secureworks Taegis NGAV」

Taegis XDRの主な特長

- エンドポイント、ネットワーク、クラウド環境をはじめとする攻撃対象領域全体をカバー
- 攻撃手法の異なる収集・監視データやイベントを機械学習／深層学習ベースで解析し、脅威インテリジェンスを適用して深掘り
- 必要なコンテキストやデータすべてが適時・適所に反映された高精度のアラート
- ワンクリックで実行可能な対応アクションと自動プレイブック
- 外部セキュリティツールとの広範囲な統合連携（プリ・インテグレーションでのご提供に加え、容易にカスタム統合可能なXDRのオープンソリューション）

Secureworks

Secureworks Taegis XDR：無料トライアル

無料トライアルを始める

高度な分析機能やデータモデリングと唯一無二の脅威インテリジェンスが融合されたクラウドネイティブソリューションTaegis XDRが、既知／未知の脅威を検知します。無料トライアルでTaegis XDRのパワーをご体験いただけます。SOC効率化のプロセスを今すぐお試しください。

上記リンクをクリックすると、Taegis XDRのパワーを実際にご体験いただけます。無料トライアルには以下の内容が含まれています。

- トライアルご登録はオンラインで完了：お支払いは一切ありません（営業担当者へのご連絡も不要です）
- おわずか数分でトライアル開始：ご登録後すぐにプラットフォームをご利用いただけます
- 任意のデータを利用可能：貴社環境における既知／未知の脅威を検知できるよう、社内データを用いたトライアルを実施していただけます
- アクセス期間は14日間です：お好きな時間に貴社のペースで進めることができます。XDRの機能をお試しください
- 事前投入済のデモデータをご利用いただけます：環境寄生型攻撃のデモデータに対するXDRの検知、調査、対応プロセスをお客様自身でご確認ください

Secureworksについて

SecureWorks®（NASDAQ：SCWX）は、20年以上にわたり実環境で蓄積された脅威インテリジェンスとリサーチに基づき構築されたクラウドネイティブのセキュリティ分析プラットフォームSecureworks® Taegis™により、高度な脅威の検知、合理化された協調モデルによる調査、また脅威に対する適切なアクションを自動的に実施する能力を強化し、お客様のビジネスを保護するサイバーセキュリティのグローバルリーダーです。

詳細は、当社のセキュリティスペシャリストにご相談ください。
☎03-4400-9373
secureworks.jp