高次元のスケール、品質、スピード

XDRの革新的な可能性

kaspersky bring on the future

XDRは誰のためのものか？

XDRは、成熟したセキュリティ体制を持つ組織向けです。インフラストラクチャ全体で発生中のすべての事象を、完全かつ体系的な全体像として把握可能な単一のプラットフォームが必要な組織にとっての選択肢となります。

世界を変える力か、痒いところに届く手か？

XDR：Extended Detection and Response

「XDR」は、多くの人々が口にする略語です。しかし、歴史が比較的浅いすべての技術の例にもれず、その正確な意味やビジネスにどう役立つのかを、知らない人々もいるでしょう。1つ確かなことは、XDRには、事後対応型から事前対応型への戦略的転換が伴うということです。「待ち」や「様子見」の姿勢は、サイバーセキュリティには役に立たないからです。XDRを単なる製品としてではなく、戦略として捉えることが賢明といえます。

では、XDRとは、痒いところに手が届くような単なる最新技術なのか、それとも世界を変える可能性を持つ技術なのでしょうか？「痒いところ」は実際に存在します。世界各国で不足しているスキル、ITセキュリティ担当者の過労、決して途切れることのない脅威の趨勢、多すぎるアラートによる心身の疲弊、ばらばらなツール、貧弱な脅威インテリジェンス、拡大する攻撃対象領域などが挙げられます。IDCは、XDRは「業界を根底から覆す力となり、SIEM、EDR、SOAR、ネットワークインテリジェンス、脅威分析プラットフォームや、外部脅威インテリジェンスのプロバイダーの売上に影響を与える[1]」と述べています。Forresterは、差別化されたXDR技術は「短期的にはEndpoint Detection and Response（EDR）に取って代わり、長期的にはSIEMを凌駕する[2]」と考えています。

「XDRは業界を根底から覆す力である」 ― IDC

デバイス、アプリケーション、ネットワークトラフィック、データ、脅威は増え続けるばかり...

XDRは誰のためのものか、そしてどんな課題を解決できるのか？

XDRは、成熟したセキュリティ体制を持つ組織向けです。インフラストラクチャ全体で発生中のすべての事象を、完全かつ体系的な全体像として把握可能な単一のプラットフォームが必要な組織にとっての選択肢となります。

こうした組織が直面しているサイバーセキュリティの課題はどこでも聞かれるものであり、定番になっています。ESG Researchは、従業員数100人以上の組織（80%以上は企業）のITおよびサイバーセキュリティのエキスパートを対象に、複数の分野を横断する調査[3]を実施しました。調査の結果のうち、重要なものを一部掲載します：

SOC技術の運用要件への適応が困難である

セキュリティ運用の管理は、過去2年間のどの時期よりも困難になっています。これは、データパイプラインの拡張性、処理エンジンの負荷分散、ストレージ容量の追加など、SOC技術の運用面でのニーズへの対応の困難さに起因します。

[1] 出典：IDC Global Security Products Analysis：From Power Point to Power Product, Where Is XDR Right Now? （2022年）

[2] 出典：Forrester, Extended Detection and Response (XDR) — A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst（2021年）

[3] 出典：ESG Research Report, SOC Modernization and the Role of XDR（2022年）

拡大と変化を続ける攻撃対象領域と脅威の全体的な趨勢

デバイス、アプリケーション、ネットワークトラフィック、データ、脅威は増え続けるばかりです。脅威の趨勢はとどまることを知らず、新たなツールが急増するにつれて、サイバー脅威の規模と複雑さも容赦なく進化しています。同時に、ハッカーの参入障壁はかつてないほど低くなっています。低スキルのハッカーがパッケージ化された脅威をダークウェブから安価で購入する一方で、高度なスキルを持つ勤勉なハッカーは複雑な攻撃を構築しています。そして、内通者による脅威と、サプライチェーンの脆弱性も忘れてはなりません。

膨大な数の手動プロセスがセキュリティ管理に必要である

収集、処理すべきセキュリティデータが増えていますが、それらを手動で処理するのは、非効率的で実効性がありません。このような運用は、最悪の事態を引き起こします。拡張性に悪影響を及ぼし、人的な直接関与に過度に依存する結果となり、脅威への対処の有効性を総じて低下させます。

脅威の検知ルールを作成できない

脅威の検知ルールを作成できない、セキュリティ管理を調整できない、迅速かつ効率的に脅威を特定し、対応することができない。これらの原因は、時間、リソース、スキルの不足です。セキュリティの分析や運用に必要なスキルや担当者が備わっていない組織も存在します。このことが、次の難題に直結します。

世界規模のスキル不足がまさに現実となっている

世界のサイバーセキュリティ担当者の数は、過去最高の470万人です。それにもかかわらず、まだ340万人が不足しており、補充する必要があります。しかし、まだ補充されていません。この格差は就労者数の2倍の速さで拡大しており、前年比26.2%の急増となっています。[4]

[4] 出典：(ISC)², Cybersecurity Workforce Study（2022年）

既存のツールでは苦労が多い

高度な脅威の検知と調査には、既存のツールを使用、管理するための専門的なスキルが必要とされます。

88%

今年、SecOpsの改善により多くの費用を投入する予定である組織のパーセンテージ

66%

ツールの統合を優先課題とする組織のパーセンテージ

目的に合致しないツール

ツール自身が問題の一部となる場合、何かが犠牲になります。既存のツールでは、高度な脅威の検知、調査に苦労することが多く、また、それらの使用と管理には専門的なスキルが必要とされます。調査[5]によると、現在のツールで行うアラートの関連付けは多くの場合効率が悪く、ITセキュリティ担当者は、連携性も共通点もない複数のツールを使用して、多種多様なデータを取り扱うことに苦慮しているとのことです。この運用は非効率的で、煩雑で、混乱を招き、経費が高くつきます。もう1つの問題は、現在のツールは、拡大を続ける攻撃対象領域に対応できるような拡張性がなく、クラウドの検知とレスポンス能力には大きなギャップがあるということです。[6]

情報セキュリティ最高責任者（CISO）がストレスを抱えるのも無理はありません。

朗報もあります。SecOpsの改善が企業の優先課題とされ、予算も確保されていることです。 88%の組織は今年、予算をさらに増やす予定であり、66%は、ツールの統合が優先事項であると回答しています。また、最近のアプリケーション開発とデプロイメントのペースはますます急速になっており、新しいスキルが必要とされています。[7]

XDRで実現できること

ここでは、XDRがこれらの課題をどう解決できるかを紹介します。

高度な脅威をより高精度で検知

XDRの脅威検知機能は、エンドポイント、ネットワーク、クラウド環境をカバーします。機械学習アルゴリズムとふるまい分析を使用して、マルウェア、ランサムウェア、持続的標的型攻撃（APT）などの高度な脅威を特定します。

自動化されたレスポンスと是正措置

XDRはレスポンスと是正措置を自動化します。これにより組織は、脅威を短時間で食い止め、想定される損害を最小限に抑制することができます。攻撃されたエンドポイントの隔離と分離、悪意がある活動のブロック、脆弱性の修正が自動化されるので、手動の作業やレスポンスの時間が短縮されます。

エンドポイント保護ツールとの統合

EPPとの統合は重要な課題です。XDRは豊富なエンドポイントのテレメトリとふるまい分析を活用して、エンドポイントの活動に対する深い見識を提供します。高度な機械学習アルゴリズムを採用し、不審なふるまいや攻撃の指標（IOA）を特定することで、巧妙な脅威を早期に検知することができるようになります。

[5] 出典：ESG Research Report, SOC Modernization and the Role of XDR（2022年5月）

[6] 出典：ESResearch Report, SOC Modernization and the Role of XDR（2022年）

[7] 出典: ESG Research Report, SOC Modernization and the Role of XDR（2022年5月）

XDRが EDR、MDR、SOAR、SIEM のエコシステムにどのように適合するか

「X」（extended）の文字が、その適合方法のヒントです。XDRはEDRが搭載する機能を拡張し、複数のインフラストラクチャレベルを横断する複雑な脅威を事前に検知します。そしてこれらの脅威に自動的に対応して阻止します。

統合的アプローチが鍵となる

複数のツールやセキュリティアプリケーションの統合と、エンドポイント、ネットワーク、クラウド、Webサーバー、メールサーバーなどの監視により、XDRによる脅威の検知と排除がさらなる効果を発揮します。同時に、製品間の対話を自動化することで、情報セキュリティの管理を簡素化します。

Forresterは、ほとんどの場合、XDRがすぐにセキュリティ分析プラットフォームに取って代わることはないと考えています。「XDRはまだ進化の途上にあり、今後5年間はセキュリティ分析プラットフォームとXDRが競合するだろう」と指摘しています。

SIEMには脅威の検知以外のユースケースもあり、SOARのカスタマイズ性は便利です。しかし、脅威の検知と対応に関しては、XDRの強力な保護機能による高度な分析は他の追随を許しません。

リアルタイムの可視性を実現

XDRは、組織のセキュリティ体制をリアルタイムで可視化します。エンドポイント、サーバー、ファイアウォール、クラウドプラットフォームなど多様なソースからのデータを収集、分析し、現在進行中の脅威や不審な活動に関する総合的な調査結果を、単一のコンソールで提供します。これにより、真の事前対応、すなわち予防的な脅威ハンティングと高速なインシデントレスポンスが実現します。全体像を把握することで、セキュリティチームは不審な活動や セキュリティインシデントの可能性をより効率的に特定できます。

データと脅威インテリジェンスを状況に合わせて活用

高品質の脅威インテリジェンスと包括的な脅威インテリジェンスデータベースを活用することで、XDRは脅威と攻撃者に関する非常に有益な背景情報を提供します。このリッチ化された脅威インテリジェンスにより、調査アラートとインシデントの処理が簡素化されます。また、脅威アクターの戦術、テクニック、動機をセキュリティチームが理解するのを支援し、より効果的なインシデントレスポンスと予防的な防御対策が促進されます。

合理化されたセキュリティ運用の実現

適切に統合された最高水準のソリューションは、現在のインフラストラクチャに容易に組み込むことができます。自動化により最高の結果をもたらし、既に使用中であるサードパーティ製ソリューションをリプレースすることなく、あらゆるデータや分析結果を可視化し、セキュリティの状況を把握できるようにします。また、セキュリティインシデントとユーザーのふるまいが総合的に可視化されるので、この統合はコンプライアンスの支援にもなるという点も見逃せません。

XDRが宣伝文句通りの性能を備えていることは明らかです：管理、安定性、加えて重要なアドバンテージはすべて実装しています。しかし、すべてのXDRが同じように開発されているわけではありません。適切なXDRは、どのように選択すればよいでしょうか？

XDRベンダーとソリューションを比較する際に考慮すべき5つのポイント

ここでは、XDRがこれらの課題をどう解決できるかを紹介します。

1

XDRソリューションの品質と、ベンダーのEPPとEDRの相乗効果には直接的な関係があります。

巧妙なサイバー脅威をエンドポイントレベルで先進的に検知し対応するEDRソリューションは、XDRの重要な構成要素です。同時に、膨大な数の脅威を自動的にふるいにかけて除外できる強固なエンドポイント保護プラットフォーム（Endpoint Protection Platform：EPP）が、EDRには必要です。エンドポイント保護の特徴をよく見極め、あらゆる種類のエンドポイント（PC、ノートPC、仮想マシン、モバイルデバイス、多様なオペレーティングシステム）をサポートしているかをチェックすることが重要です。

2

最新の脅威インテリジェンスおよびサイバー犯罪者の戦術やテクニックの全貌の把握が、サイバー脅威への対抗に不可欠

それほど難しいことではありません。優れたXDRソリューションであれば、インシデントの調査とレスポンスを改善しスピードアップするための付加的な背景情報を入手しつつ、上記2つの条件を満たすことが可能です。

3

高い持続性と費用対効果を備えつつサードパーティ製ソリューションと統合

XDRソリューションとサードパーティ製ソリューションの統合の品質は、極めて重要なもう1つの課題です。これらの相互運用が可能であれば、ソリューションの購買は最初から持続可能な投資となるからです。数多くの信頼できる統合オプションを実装するXDRソリューションは、より多くのデータソースからデータを収集し、インフラストラクチャで現在発生している事象の全体像の全体像の完全性をより高めて提供します。

4

第三者によるレビュー、国際的な認知度、第三者によるテスト結果が重要

サイバーセキュリティのように、ビジネスにとって重要となるものに投資する際は、第三者による評価結果を見逃してはいけません。第三者機関によるテストの結果を確認しましょう。ForresterやIDCなど、国際的な評価もチェックしてください。そのソリューションは、世界各国で実装されていますか？ケーススタディにも目を通しましょう。

5

将来を視野に入れて投資していますか？

技術の進化は止まることがありません。特に、比較的歴史が浅いXDRのような技術の場合は、継続的な開発に向けてベンダーのロードマップがどのようになっているかを見極める必要があります。

Kasperskyを選ぶ理由

最多のテスト回数。最多のトップ評価獲得実績。それがKasperskyの保護です。

Kasperskyは、セキュリティを専門分野として多くの実績を積み重ねてきたグローバルなサイバーセキュリティ企業です。世界各国の組織を保護してきた実績は25年以上におよび、当社の製品とサービスは数えきれないほどの受賞実績があり、称賛を受けています。2013年から2022年までに、Kaspersky製品が達成した実績は次の通りです：

587

1位の獲得回数587回

685

トップ3の達成回数

827

第三者評価機関が実施したテストやレビューに参加した回数

2023年、世界有数のテクノロジーリサーチ&アドバイザリー企業であるISGにより、KasperskyはXDRソリューション市場のリーダーであるとされました。ISGの定義によると、「リーダー」とは、総合的な製品とサービスを提供し、力強いイノベーションと安定した競争力を示す存在です。

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture