kaspersky BRING ON THE FUTURE

XDR vs SIEM vs SOAR

略語が多すぎて混乱する？これらの短い文字の裏に何が潜んでいるか見ていきましょう。

はじめに

SIEM、SOAR、MDR、EDR、EPP、XDR... サイバーセキュリティの略語のジャングルで迷子になって困惑していませんか。無理もありません。そこで、SIEM、SOAR、XDR という大物 3 つの違いを解明するのに役立つガイドをご用意しました。これらの略語の裏には何が隠れているのでしょうか。業界ではこれらの紛らわしく意味も重なる用語をどのように生み出したのでしょうか。それぞれに何かはっきり異なる意味などがあるのでしょうか。それとも単なるマーケティング戦略でしょうか。どのような類似点や違いがあるのでしょうか。相互補完ができるのか、それとも互いに競合しているのでしょうか。

一緒に探求してみましょう。知識のナタを振り上げて、略語や業界用語の森を切り開き、明確な理解が広がるオープンスペースに到達しましょう。

SIEM

セキュリティ情報イベント管理（SIEM、Security Information and Event Management）は、セキュリティイベント管理（SEM、Security Events Management）とセキュリティ情報管理（SIM、Security Information Management）を 1 つのプラットフォームにまとめたツールとサービスのセットです。SIEM は、ガバナンスとコンプライアンスや、疑わしいアクティビティを照合するルールベースの関連付けといった様々なユースケースのログデータを IT インフラストラクチャ全体から収集、集約、分析、保存します。

SIEM の仕組み

最初の SIEM サービスは、さかのぼること2005 年に開発されました。もともとの目的は、コンプライアンスレポート作成のために、企業の IT インフラストラクチャ全体（エンドポイント、アプリケーション、ネットワークデバイスなど）からログとイベントを集約して保存することでした。SIEM では、このデータセットで関連付けを実行して、疑わしいふるまいを示すパターンまたはイベントを探し、セキュリティオペレーションセンター（SOC）向けのアラートを生成します。セキュリティアナリストは、これらのアラートを、コンプライアンスとガバナンスの目的だけでなく、エコシステムで悪意のあるアクティビティをプロアクティブに特定してその進行を停止するために使用できそうだとすぐに気づきました。

SIEM の限界

問題は、SIEM サービスが、インシデントの検知と対応に特化した設計ではなかったことでした。このため、この目的で使用するのは、以下のような多くの理由で、少し困難でした：

- アラートが多すぎる — SIEM が提供する大量のデータセットは、手動でのフィルタリング、処理、分析が必要でした。これは、脅威が急速に変化する状況で攻撃を防ごうとしているセキュリティアナリストにとっては不都合でした。
- コンテキストがない — 複雑で高度な新しい攻撃に対処するためにセキュリティアナリストが必要としているのは、SIEM によって提供されるばらばらのデータストリームではなく、組織の脅威の状況を示す、コンテキストに基づく整合の取れた全体像です。
- 受動的すぎる — 疑わしいプロセスのブロック、ファイルの隔離、その他の対応機能は、このサービスには含まれていません。これは基本的に受動的なデータ分析ツールだからです。

セキュリティの専門家は、SIEM の上に追加のツールを重ねたり、機械学習やふるまい分析のプラグインを含む新たな世代を開発したりして、これらの問題を解決しようとしてきました。しかし、質の高いアラートや高速な自動プロセスを備えた機能を提供するツールに対する要求は残りました。

SOAR

セキュリティオーケストレーション、自動化、対応（SOAR、Security Orchestration & Automated Response）ツールは、上で挙げた SIEM システムの欠点のいくつかを解決するため、2015 年に登場しました。SOAR プラットフォームは、管理システムや脅威インテリジェンスプラットフォームを含むインフラストラクチャ全体の様々なソースからデータを取得し、優先度分析を提供します。次に、セキュリティチームは、SOAR プラットフォームでセキュリティツールが API 接続された統合エコシステムを使用して、侵入する脅威に対して、多段階でクロスソリューションの自動対応を設定できます。

SOAR の仕組み

これについては名前が大きな手がかりになります。その理由をご説明します。

SOAR ツールでは自動化を行います。インシデント対応プロセスを自動化する機能が最もよく知られていますが、これらのツールは、実は脆弱性スキャン、ログ分析、ユーザーアクセス管理、脅威トリアージなど多くの幅広いワークフローを自動化できます。

これを行うには、事前設定済みのルールセットである「プレイブック」が使用されます。これは、特定のイベントによってトリガーされ、システムに特定のワークフローで次に取るべきステップを伝えます。ほとんどの SOAR ソリューションには、すぐ使用できる数百のプレイブックが用意されており、SOC チームが直面する一般的なタスクをカバーしています。さらに、チーム独自のプレイブックを設定して、他に実施する特に繰り返しの多いプロセスがあればそれを自動化できます。

次は、オーケストレーションです。自動化は、1 つのフロー内の個別タスクを機械で実行することですが、オーケストレーションは、複数の異なるツールやプロセスをより大きいワークフローで連携させることをいいます。これによって関連するすべてのデータを 1 つのプラットフォームにまとめて統合された実行性の高い情報を得ることができます。

SIEM と SOAR の関係

一般に、SIEM は、SOAR ツールと併用され、アシスタントとマネージャーのような関係になっています。SIEM は、すべてのログを収集し関連付けてアラートを見つけ、この情報を SOAR に提供します。対応アクションは SOAR が主導できます。

SOAR の限界

ここまでの話では、非常によさそうに思えます。問題は、パートナーツールを統合する適切な設定の SOAR プラットフォームの管理には、高いスキルを持つ熟練した SOC の不断の努力が要求されることです。しかし、現在のサイバーセキュリティスキルのギャップから考えると、そのようなリソースを現在保持している組織は多くありません。

そのように高いスキルで常時警戒する管理ができない場合、SOAR アナリストは、結局、サイロ化された様々なツールからプラットフォームに吐き出される優先度の低いアラート、誤検知、全体的につじつまの合わないデータセットに悩まされることになります。これはまさにアナリストが避けようとしていたことです。

XDR

XDR は、オンプレミスまたはクラウドベースのセキュリティソリューションで、ネイティブとハイブリッドの 2 つのカテゴリに大別されます。ネイティブ XDR は、単一ベンダーの統合ツールセットです。一方、ハイブリッド XDR は、エコシステムに他の複数のサードパーティソリューションを統合したものです。「XDR」という用語が最初に使用されたのは 2018 年で、「X」は「eXtended（拡張）」の略です。XDR は、複数のセキュリティ層（メール、クラウド、ネットワークなど）のデータを収集して関連付けて IT インフラストラクチャ全体の包括的な保護を提供することで、従来のエンドポイント検知、対応、保護ツール（EDR および EPP）を「拡張」します。

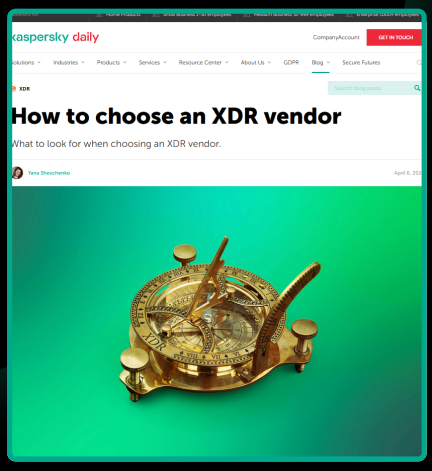
つまり、これは、様々なツールを連携させ、機械学習と自動化を使用して、セキュリティチームによるセキュリティエコシステム全体の保護を支援する単一のプラットフォームです。SOAR の説明で聞いたような話ですね。しかし、いくつか根本的な違いがあります。ご説明しましょう。

XDR と SOAR の違い

1. XDR ソリューションは、エンドポイントのデータと最適化に固定されています。つまり、インシデントの検知と対応が設計の中心的な機能であり、高度な分析が可能です。これは通常 SOAR ツールにはありません。XDR ツールは、未知の脅威やゼロデイ脅威の検知を得意としており、強力な人工知能、機械学習アルゴリズム、脅威インテリジェンスを活用して、組織をその境界を越えて守ります。一方 SOAR ツールは、より幅広いユースケースに対応できます。インシデント対応だけでなく、インフラストラクチャ全体のあらゆるプロセスのオーケストレーションと自動化が可能であるからです。
2. XDR は、SOAR の軽量版といえるもので、侵入してくる脅威やアラートに対して、ワンクリックで自動対応できる効率的なインターフェイスを備えています。適切に設定された複雑な SOAR プラットフォームを管理するリソースがない組織にとっては、XDR のほうがはるかに便利です。
3. XDR では、複数製品にまたがる統合もスムーズです。これは 単一ベンダーのツールスタックでも、複数のサードパーティ製品でも同様で、シームレスな相互運用の点で優れています。SOAR ツールでは、サイロ化された異なるツールをすべてスタックに統合するのが難しい場合が多いですが、XDR は、効率的なオールインワンの脅威対応のためにこれらのサイロを分割します。

XDR ベンダーの選び方

多くのサイバーセキュリティベンダーが XDR の時流に乗って独自のソリューションを提供しています。どうすれば妥当な製品かどうかを判断できるでしょうか。有用な方法をガイドから参照してみましょう：
https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



SIEM と SOAR は XDR に置き換わるのか

これについてはまだ結論は出ていません。XDR がまだ開発が続いている比較的新しいテクノロジーであるためです。各ソリューションには他を補完するメリットがあるので、現在、ほとんどの専門家は統合アプローチを推奨しています。

- SIEM — SIEM は、ログ管理、コンプライアンス、脅威以外の関連データの分析など、脅威検知以外のユースケースに役立ちます。
- SOAR — SOAR プレイブックは細かいカスタマイズが可能なので、組織のインフラストラクチャ全体でプロセスのオーケストレーションと自動化を行う場合に便利です。
- XDR — 脅威の検知と対応に関して言えば、XDR ソリューションは、その高度な分析によって他とは比べものにならない強力な保護を提供できます。

社内の専門家向けに、十分テストされた適用可能なソリューションをお探しですか。

Kaspersky Expert Security は、クラウドネイティブの EDR ソリューションをベースにした XDR であり、すべてのエンドポイントとネットワークを対象に、AI ベースの検知と自動対応ロジック用に強化された可視性と機能を提供します。これによって、多様な自動インシデント対応のシナリオを容易に処理できます。プラットフォームに組み込まれた高度な検知と分析のテクノロジーは、世界トップレベルの脅威インテリジェンスで補完されます。カスペルスキーの XDR の統合アーキテクチャは、単一の Web コンソールから集中管理できます。詳細は、次を参照してください：
go.kaspersky.com/expert

www.kaspersky.co.jp