ホワイトペーパー

オープンXDR vs. SIEM

リソースとビジネスリスクを適切なソリューション
と一致させる

STELLAR CYBER®

可視性を獲得し、エンタープライズインフラストラクチャ全体（エンドポイント、サーバー、アプリケーション、SaaS、クラウド、ユーザーなど）にわたる攻撃に対応することは、今日のサイバーセキュリティ環境では非常に困難な作業です。企業は、この課題に対処するために、SIEM、UEBA、SOAR、EDR、NDR、TIP、およびその他のツールで構成される複雑なセキュリティスタックを作成することを余儀なくされています。 多くの企業にとって、SIEMはインフラストラクチャからのデータを集約および分析するための主要なツールです。企業のほぼ半数がSIEM(1)に満足していないと報告していますが、すべての企業は、SIEMの立ち上げと維持に費やした資本、時間、およびリソースの量をすぐに指摘します。オープンXDRは、企業インフラストラクチャ全体にわたる可視性の獲得と攻撃への対応という課題に対処する新しいアプローチとして浮上しています。この記事では、オープンXDRとSIEMがセキュリティソリューションとしてどのように評価されるかを見ていきます。

オープンXDRの定義

ガートナーは、XDR（eXtended Detection and Response）を、「複数の独自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相互に関連付ける統合セキュリティインシデント検出および応答プラットフォーム」と定義しています。2020年にさかのぼるこの定義は、オープンXDRを、プロプライエタリまたは単一ベンダーのコンポーネントだけでなく、既存のすべてのセキュリティコンポーネントからデータを収集して相互に関連付けるXDRの新しいカテゴリとして捉えていません。したがって、オープンXDRは、「オープンアーキテクチャを介して提供されるすべての既存のセキュリティコンポーネント」で終わることを除いて、ガートナーのXDR定義と同じように定義されます。オープンXDRとネイティブXDRの違いについては、別の記事で詳しく説明しています。この記事では、SIEMと比較してオープンXDRに焦点を当てます。したがって、オープンXDRには、上記の定義の約束を満たすために、次の技術要件があります。

- **デプロイ可能性** – スケーラビリティ、可用性、およびデプロイメントの柔軟性を実現するクラウドネイティブのマイクロサービスアーキテクチャ
- **データ融合** – ネットワーク、クラウド、エンドポイント、アプリケーション、IDを含む攻撃対象領域全体でデータを一元化、正規化、強化
- **検出** – 機械学習による組み込みの自動検出
- **相関** – 複数のセキュリティツールにわたる忠実度の高い相関検出
- **インテリジェントな応答** – 同じプラットフォームからのワンクリックまたは自動応答

SIEMに少しSOARを加えたものに似ていますか？ それはそうだからです。 ただし、Open XDRが、SIEMが不足しているSIEMの多くの約束を実現できるようにする、アーキテクチャ上の大きな違いがあります。

SIEMの定義

ガートナーは、SIEM（Security Information and Event Management）を、「セキュリティイベント、およびその他のさまざまなイベントの収集と分析（ほぼリアルタイムと履歴の両方）を通じて、脅威の検出、コンプライアンス、セキュリティイベントの収集と分析（ほぼリアルタイムと履歴の両方）、およびその他のさまざまなイベントとコンテキストデータソース」と定義しています。この定義は、XDRの定義と特に似ています。アーキテクチャには最大の違いがありますが、純粋に定義上、SIEMはその主な目的（情報とイベントを管理すること）にちなんで名付けられました。XDRは、その主な目的である検出と応答にちなんで名付けられました。これは些細なことのように思えるかもしれませんが、ビジネス目的のこの違いがアーキテクチャアプローチを推進するものであり、SIEMが今日のセキュリティ環境で非常に資本集約的である理由です。

アーキテクチャの比較

この比較は、違いのみに焦点を当てています。長期的なストレージ、セキュリティツールとのオープンな統合、クラウドのネイティブ性、効率的な検索と脅威のハンティングなど、多くの技術的な類似点があります。 ただし、オープンXDRには、SIEMとの5つの重要なアーキテクチャ上の違いがあります。

1. データは強制的に正規化された濃縮状態になります。これは、データがデータレイクに保存される前に行われます。
2. アラートの検出と相関は、SIEMのように人間が作成したルールではなく、オープンXDRのAI

によって自動的に駆動されます。

3. インシデントは相関アラートから生成され、同じプラットフォーム上の単一の応答が調整されます。SIEMは、別のSOARプラットフォームにアラートを送信し、その後、ダウンストリームの相関と応答を実行します。
4. ビッグデータレイク、UEBA、SOAR、TIP、NDR、EDRなどのセキュリティ運用に必要な多くのツールが1つのプラットフォームに統合されていますが、多くのSIEMにはビッグデータレイクしか含まれていないため、SIEMユーザーは多くの複雑なツールを手動で組み合わせる必要があります。

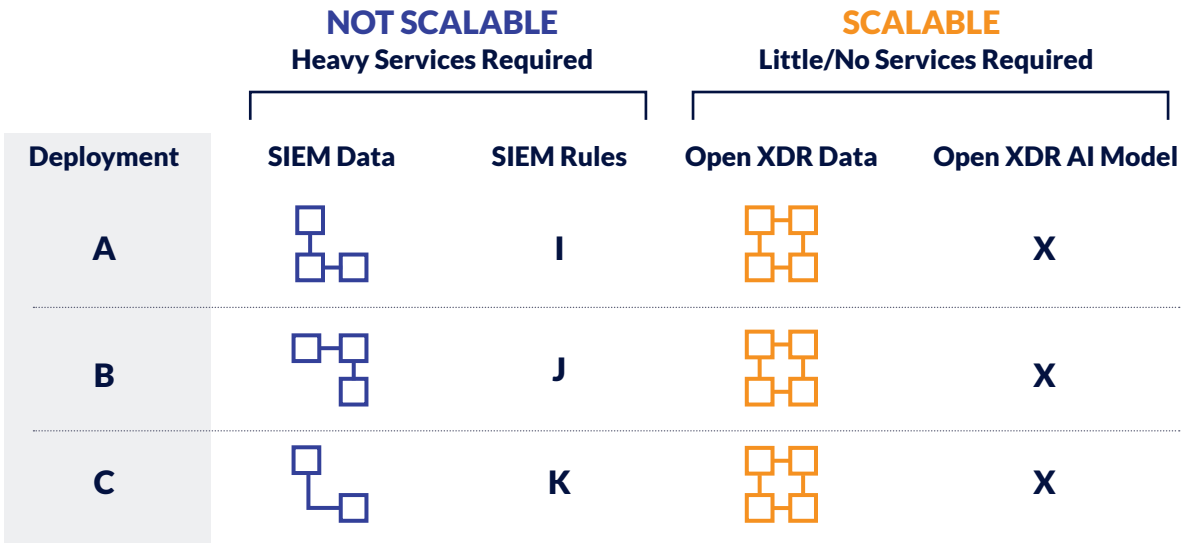
違い1と2は密接に関連しています。あらゆる業界で意味のあるAIを構築して維持するには、データの問題を解決する必要があります。セキュリティでは、データの複雑さを軽減するために、データを一元化、正規化、および強化する必要があることを意味します。プラットフォームの展開ごとにデータのモデルが異なる場合、AIモデルを維持することは不可能な問題になります。XDRは、データがデータレイクに到達する前に、各展開で同じ方法でデータをモデル化するように強制します。データは、正規化された濃縮状態でのみ利用できます。SIEMは、これをオプション機能として提供するか、この機能をまったく提供しません。オプションの場合、正規化とエンリッチメントは、すでに保存されている生データに対する後処理ステップとして扱われます。

要約すると、技術的な違い1と2について、オープンXDRはデータの正規化と強化を強制するため、イベントとアラートを相互に関連付ける意味のあるAIを構築できます。同じ理由で、SIEMアーキテクチャは、データを処理するため、同じ忠実度のAIエンジンを生成できません。SIEMはAIを活用できますが、スケーリングは困難です。

技術的な違い3は、同じプラットフォームで相関と応答を実行するオープンXDRにあります。インシデントの高次構造（複数の関連するアラート）は、オープンXDRプラットフォームで自動的に生成され、全体的に応答されます。SIEMはアラートをSOARに渡す必要があります。SOARは、環境内で発生するすべての詳細なコンテキストなしで、アラートをルールと相互に関連付ける必要があります。オープンXDRは、SIEMやSOARと同じように応答を生成しますが、すべてのデータが利用可能な検出とAI駆動の相関を実行する同じプラットフォームから調整されるため、応答の忠実度はXDRの方がはるかに高くなります。

最後の技術的な違いは、全体的なセキュリティスタックを構築および維持するためのアプローチに集中しています。オープンXDRは、セキュリティ操作のためのすべての主要なツールを統合して、1つのプラットフォームから調整できるように設計されています。多くのSIEMは、プラグインの長いリストと詳細なレベルのカスタマイズを提供しますが、それはユーザーにシステムの構築と構成の責任を負わせます。

企業にとって、これらの技術的な違いは、セキュリティプラットフォームを実行するために必要



な資本、時間、およびリソースに影響を与えます。SIEMはオープンエンドのテクノロジーであるため、運用に費用がかかります。オープンXDRプラットフォームはセキュリティの規範的なテクノロジーであるため、企業はそれらを採用する際にはるかに効率的になります。

最後に、厳密には技術的な違いではありませんが、SIEMがはるかに重点を置いている2つの領域は、コンプライアンス関連の大量のストレージとIT運用のための同じプラットフォームの使用です。XDRは、検出と応答の結果のために設計されています。それでもコンプライアンス要件を満たすことができますが、最初からそのために設計されていませんでした。オープンXDRはセキュリティに厳密に焦点を当てているため、同じプラットフォームでのIT運用は、SIEMだけが主張できるものです。

NG-SIEMはどうですか？

「次世代」とは、違いではなく、より良いものを示すものです。NG-SIEMは、仮説的な意味でSIEMよりも優れています。オープンXDRは両方とは異なります。NG-SIEMは、レガシーSIEMが今日のセキュリティ環境の要求に追いついていない多くの分野で大きな進歩をもたらしました。注目すべき改善点は次のとおりです。

- ビッグデータテクノロジーの使用（SIEMが絶えず転倒することはもうありません）
- さまざまなアルゴリズムによる一部のユーザーおよびエンティティの行動分析（UEBA）
- 脅威ハンティングなどの主要なワークフローに対するUI / UXの改善
- SOARとのネイティブまたはオープン統合
- データモデリングプラグイン

NG-SIEMは、オープンXDRとSIEMの間の機能のギャップを確実に埋めますが、アーキテクチャの違いは同じままです。

一部のベンダーは、SIEMとXDRプラットフォームを提供していると述べています–何が得られるのでしょうか？

上記のように、SIEMとオープンXDRの間には多くの類似点があります。技術的な違いは微妙ですが、事業価値と運営に必要な資本に大きな影響を及ぼします。SIEMとオープンXDRの両方を使用して製品を説明している場合、ベンダーは2つの主張をしています。ベンダーが最初に主張するのは、「SIEM機能」を使用して、SIEMのすべての重要な機能（オープンコレクション、ストレージ、検索、レポート、クラウドネイティブ）を備えたオープンXDRプラットフォームを参照する方法を説明する方法です。オープンXDRは、特に既存のSIEMを置き換えるために、エンタープライズセキュリティスタックに展開できます。

ベンダーが主張する可能性のある2番目の主張は、自社のプラットフォームがSIEMとオープンXDRプラットフォームの両方であると言うことです。これは、ベンダーが潜在的なカテゴリマーケティングを見逃さず、SIEMまたはオープンXDRのどちらを探しているかに関係なく、顧客に製品を販売できるようにするための紛らわしい点です。ただし、前述のように、SIEMとオープンXDRは異なるため、同じ製品を両方にすることはできません。

XDRとSIEMの衝突コースをナビゲートする

Forrester2が指摘しているように、XDRはSIEMおよびSOARとの衝突コースにあります。企業は、長期的なビジネス成果と利用可能なリソースを念頭に置いて、両方のテクノロジーカテゴリにアプローチする必要があります。箱から出してすぐに使用できる、忠実度の高い自動検出と応答の方が重要ですか？ 同じチームによる同じプラットフォームからの応答能力は、攻撃の滞留時間を短縮するために重要ですか？ チームのスタッフが不足しているか、ツールを実行するために多くのトレーニングが必要ですか？ これらは、セキュリティスタック戦略を定義し、XDRとSIEMのどちらが適切かを判断する際に、企業がテーブルに持ち込む必要のある重要な質問です。

[1] 2017 Ponemon SIEM Report

[2] https://www.forrester.com/report/Adapt+Or+Die+XDR+Is+On+A+Collision+Course+With+SIEM+And+SOAR/-/E-RES165775