ホワイトペパー

オープンXDRの事例

Xは全てを意味します

STELLAR CYBER®

サイバーセキュリティの現在のモデルは壊れています。これは、ログやトラフィックを分析し、脅威となる可能性のある異常を検出するために、それぞれが独自のコンソールを備えた多数のスタンドアロンツールを取得して展開することで構成されています。このモデルでは、各セキュリティアナリストが他のアナリストと通信して、各ツールの個々の検出（それぞれがそれ自体は無害に見える可能性があります）が他のツールからの他の検出と相関して複雑な攻撃を明らかにできるかどうかを判断する必要があります。

このモデルにより、企業は、企業のインストルメンテーション、脅威の特定、脅威への対応、およびリスクの管理を目的として、SIEM、SOAR、EDR、NDRなどで構成される複雑なセキュリティスタックを作成する必要があります。これらすべてのツールの取得とライセンスの管理は複雑で費用がかかり、各ツールの検出を比較するために必要な手動の相関関係により、セキュリティインフラストラクチャ全体に多くのギャップが残ります。

アナリストは、これらのシステムによっても誤検知が発生することが多く、「アラート疲労」と仕事の不満を引き起こします。既存のSIEMやその他のツールに満足していると宣言する企業でさえ、マルチツールセキュリティインフラストラクチャの立ち上げに費やした時間とエネルギーが必要な結果をもたらしていないことを認めます。

XDRの事例

XDR（eXtended Detection and Response）は、頭字語ではXが実際には変数であるため、検出と応答を実行するすべてのテクノロジーの包括的な定義になっていますXは「Endpoint +」または「Network +」を表すことができますが、これは、サイロ化されたツール、相関のないデータ、およびアラートの疲労という企業の現在の苦痛を無視します。XDRの全体的な目標はこの痛みに対処することであるため、Xは「全て」を意味する必要があります。 したがって、全ては、検出と応答を通じて攻撃対象領域全体をカバーするプラットフォームアプローチを意味します。

このプラットフォームアプローチは、サイロ化されたツールを統合ツールセットに変換し、無相関データを攻撃対象領域の生きた相関表現に変換し、アラート疲労を安心に変換することで、今日の壊れたモデルを修正できます。テクノロジーがこの目標をどのように実現するかが、アーキテクチャ上の重要な問題です。今日のXDRには、オープンとネイティブの2つのタイプがあります。

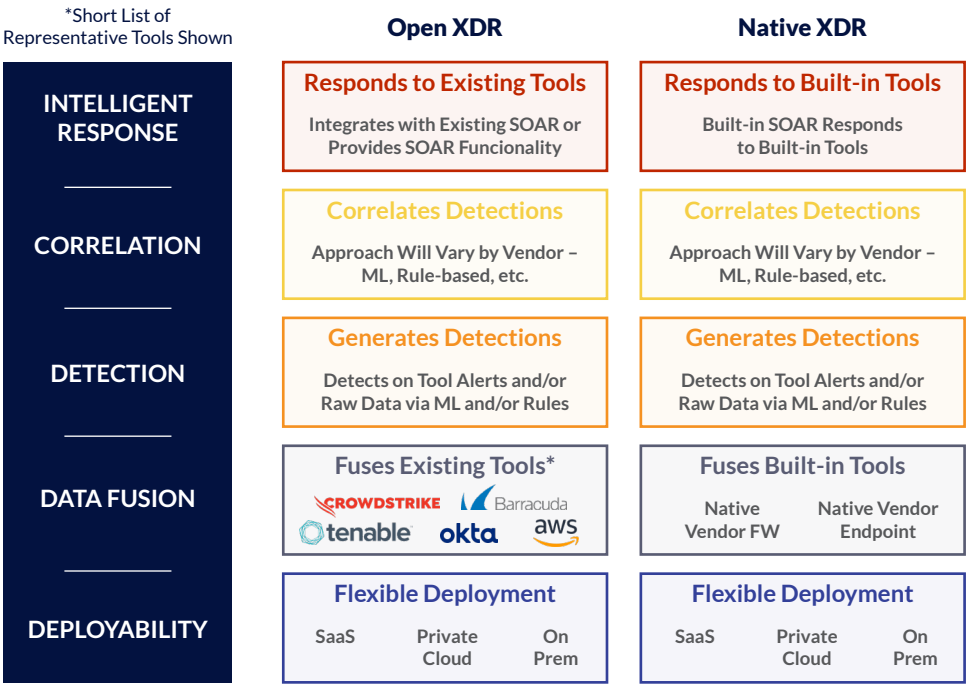
オープンXDRとネイティブXDR

- オープンXDRは、攻撃対象領域全体で既存のセキュリティツールのテレメトリおよび応答機能を活用できるオープンアーキテクチャを介して提供されます
- ネイティブXDRは、攻撃対象領域全体でテレメトリと応答を提供する単一ベンダーのセキュリティツールスイートから提供されます

Regardless of the architectural approach
XDRプラットフォームのアーキテクチャ上のアプローチに関係なく、XDRと見なされるには、次の技術要件を満たす必要があります。

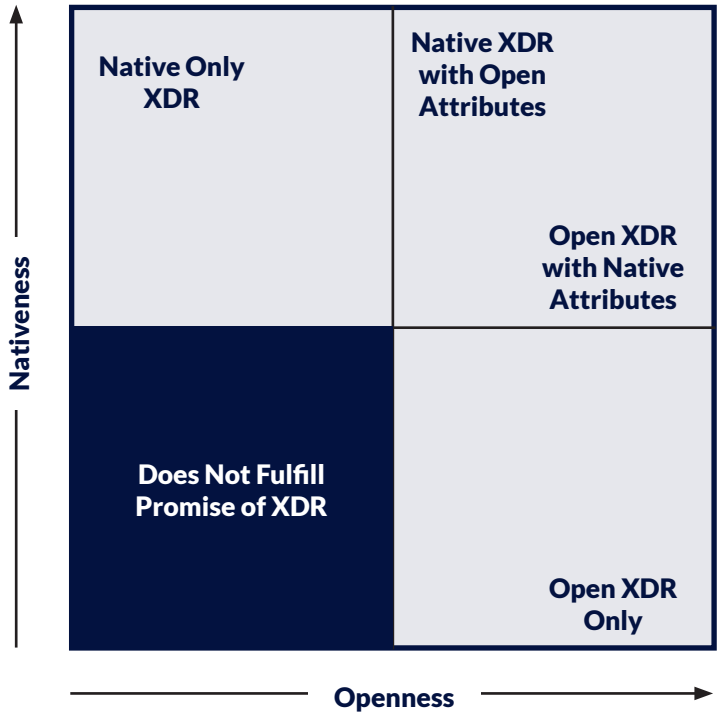
- **デプロイ可能性 –** スケーラビリティ、可用性、およびデプロイメントの柔軟性を実現するクラウドネイティブのマイクロサービスアーキテクチャ
- **データ融合 –** ネットワーク、クラウド、エンドポイント、アプリケーション、IDを含む攻撃対象領域全体にわたる正規化および強化されたデータ
- **検出 –** 複数のセキュリティツールにわたるリアルタイムの忠実度
- **相関 –** コンテキストアウェアインシデントをもたらす相関検出
- **インテリジェントな応答 –** 同じプラットフォームからのワンクリックまたは自動応答

XDRアーキテクチャの比較



オープンXDRとネイティブXDRに関する一般的な誤解は、それらが相互に排他的なタイプのXDRであるというものです。または、そうではありません。XDRプラットフォームは完全にオープンで、部分的にネイティブにすることができます。たとえば、XDRプラットフォームには、他のベンダーの既存のツールとオープンに統合しながら、そのベンダーのいくつかの組み込みツールを含めることができます。これにより、コンポーザブルセキュリティ戦略が可能になります。これは、既存のツールを活用しながら、お客様が適切と思われる時間と場所でツールの一部を廃止できるようにする機能です。

XDRの寸法



プラットフォームがそのアプローチで採用するオープンXDRとネイティブXDRの構成は、目的を達成するための手段です。具体的には、プラットフォームが攻撃対象領域全体で検出と応答を実行する方法です。XDRの購入者は、アーキテクチャアプローチを目的を達成するための手段と見なし、企業にとって最善の決定を下す必要があります。

理想的なXDRはオープンです

セキュリティスタック全体を単一のベンダーに移行し、閉じたネイティブXDRプラットフォームを採用しても問題がない企業もあります。たとえば、攻撃対象領域全体をカバーすることをあまり気にせず、エンドポイントの検出と応答のみを必要とする企業もあります。この場合、EDRベースのネイティブXDRプラットフォームを追求する必要があります。

ただし、ほとんどの企業では、オープンXDRプラットフォームを最優先事項と見なす必要があります。どうして？ 単一のベンダーが最高のクラウド、エンドポイント、ネットワーク、IDなどのツールを作成または取得することはできないため、ネイティブのみのXDRプラットフォームは最善の方法ではありません。さらに、企業が既存のセキュリティツールの展開にすでに多額の資本と労力を投資している可能性が非常に高いです。これらの投資を放棄したくないため、クローズドなネイティブXDRソリューションはこれらのツールと相互作用せず、相互作用しません。その企業の攻撃対象領域全体をキャプチャします。オープンXDRプラットフォームに、成長する企業の攻撃対象領域の特定の領域をカバーするネイティブ属性がある場合は、すばらしいです。 ただし、最初にオープンにする必要があります。

結局、企業がコンポーザブルセキュリティ戦略を定義して実行し、プラットフォームを通じてXDRのすべての技術要件を実現したい場合、完全にオープンなXDRプラットフォームが唯一の現実的な方法です。