2022年に注目すべきSIEMの5つの動向

splunk>
turn data into doing®

SIEM(セキュリティインシデント/イベント管理)テクノロジーは何年も前から存在していましたが、そのプラットフォームの中核的な機能の登場は10年以上前に遡ります。それ以降、SIEMソリューションはログ管理ツールから情報プラットフォームへと進化し、SIEM市場の大部分が企業ニーズによって牽引されています。このわずか数年で、SIEM市場は20億ドルから41億ドルという規模にまで成長しました。

また、大手市場調査会社の調査では、データ侵害のコストが2024年までに5兆ドルを超える可能性があることが判明しました。これは2019年に報告された金額(合計3兆ドル)のほぼ**2倍**です。しかし、SIEMソフトウェアの最新機能のおかげで、組織はこの種のリスクを軽減し、深刻な被害が発生する前に(すべてではないにせよ)ほとんどの脅威を阻止することができます。ベンダーによるSIEMソフトウェアのイノベーションや改善が継続的に行われていることから、ガートナー社のSIEM (セキュリティ情報/イベント管理)部門のマジック・クアドラントでは、これらの動向に注目しています。

数多くの優れた機能が登場していますが、2022年に注目すべきSIEMの5つの動向は次のとおりです。

1. クラウドとアプリケーションのセキュリティが最優先事項であり続ける。
2. リスクベースのアラートへの注目が高まる。
3. 脅威インテリジェンスと製品内のセキュリティコンテンツは、今や不可欠である。
4. 自動化により、効率、生産性、対応が向上する。
5. 内部不正、内部脅威の特定と対応が容易になる。

01

クラウドとアプリケーションのセキュリティが最優先事項であり続ける

新型コロナウイルスの感染拡大やリモートワークへの大規模な移行によってクラウドの導入が進む中、あらゆる規模の企業にとって最新のセキュリティソリューションが不可欠なものとなっています。企業が驚異的なスピードでクラウドに移行し始めたり、多くの組織がクラウドインフラストラクチャへの移行を進めるにつれ、クラウド戦略の強化と整備の必要性がさらに増してきています。

移行の技術的な複雑さは、クラウドネイティブに移行する際に直面する課題の1つに過ぎません。各部署がデジタル化を急ぎ、競合他社に打ち勝つため、また優先順位の変化に対応しようとすると、一般的なセキュリティ要件を見過ごしてしまいがちです。このことは、最終的にリスクの増加につながります。特にネットワーク制御、アクセス管理システム、クラウド構成オプションが最新の状態になっていない場合は深刻です。

さらに、攻撃対象の拡大や可視性の欠如といった要因が重なれば、侵害のリスクは目前に迫っているといえるでしょう。だからこそ、堅牢なSIEMソリューションには、あらかじめ定義されたセキュリティ監視コンテンツが用意されています。このコンテンツを活用すれば、ハイブリッド環境、クラウド環境、マルチクラウド環境での脅威の検出と対応が容易になります。また、このようなSIEMには、クラウド攻撃に対する高度な検出ルールや、クラウドでの検出を継続的にテストして改善するための広範囲なクラウド攻撃範囲も含まれます。

このリモートワークの時代には、量、種類、速度に関係なく、クラウドとエンドポイントのすべてのデータを取得して分析できるSIEMソリューションが必要です。従来の監視方法ではもはや不十分です。セキュリティチームは、セキュリティイベントが発生した場所と原因を検出するために、あらゆる環境のさまざまなソースからのデータを取り込んで分析する必要があります。

02

リスクベースのアラートへの注目が高まる

過剰なアラートは毎日のようにアナリストを悩ませ続けています。さまざまな定義によって検出されたアラートは、セキュリティオペレーションセンター (SOC)内で大量の誤検知と多くの余分なノイズを生み出すため、最前線の担当者はすぐに圧倒され、過度な負担を強いられます。

当然のことながら、SIEMでは標的型攻撃と侵害の検出、対応をより効果的に行う必要があります。リスクベースのアラート(RBA)は、脅威を特定するための新しい方法であり、リスクの原因をユーザーとエンティティに関連付け、特定の行動やリスクのしきい値を超えたらアラートをトリガーします。

セキュリティチームは、アラートの量を減らすと同時に真陽性を増やすことができるため、従来のサーチでは見逃されがちだったより巧妙な攻撃を検出できます。

SIEMの行動プロファイリング、脅威インテリジェンス、および分析機能を使用すれば、複雑で精度の高い脅威に時間とリソースを費やせるようになり、検出の成功率を飛躍的に向上させることができます。また、アナリストは、MITRE ATT&CKやNISTフレームワークなどの業界標準のサイバーセキュリティフレームワークに照らして、リスクの原因をさまざまなエンティティに関連付けることもできます。

03

脅威インテリジェンスと製品内のセキュリティコンテンツは、今や不可欠である

セキュリティプログラムのルールを管理しながら進化させることは簡単ではありません。多くのさまざまなソースがあり、選別するデータ構造や形式も多岐にわたるため、必要なインテリジェンスを利用するには手間と時間がかかります。セキュリティチームに必要とされる検出ルールやプレイブックを作成するための余力がほとんどあるいはまったくない場合は、これが特に顕著になる可能性があります。

しかし、今日の最新のSIEMソリューションは、脅威インテリジェンス(既存および新たな脅威に関する製品内のセキュリティ調査など)をインシデント対応フローの各段階に統合することも、チーム、ツール、同業他社、パートナーのエコシステムと統合することもできます。このようなサポートにより、ユーザーはバックエンドでスクリプトの作成や保守を行うことなく、攻撃を未然に食い止めたり、複雑なパイプラインを作成したりすることができます。

最後に、急成長を遂げるインテリジェンス市場(オープン、商用、コミュニティのあらゆる種類のインテリジェンスソース)のおかげで、アナリストがアラートの調査や対応を行う際に段階的に使用できる最新の技術ガイダンスやコンテキスト認識(攻撃の背後にいる人物やその手法など)を、SIEMソリューションに組み込めるようになりました。

04

自動化により、効率、生産性、対応が向上する

セキュリティタスクの中には、チームが手動で処理するには規模が大きすぎて面倒なものがあります。また、セキュリティスキルの不足により、組織のワークロードに見合った人材を見つける(ましてや雇用する)ことが困難であることは言うまでもありません。当然のことながら、アナリストが疲弊してしまい、差し迫っている脅威を見逃してしまうこともあります。生産性、効率、スピードを最大化するため、そして誰もが健全さを失わないようにするための唯一の打開策が自動化なのです。

セキュリティのオーケストレーションと自動化によるレスポンス(SOAR)のトピックに移りましょう。現在、ほとんどのSIEMソリューションでは、SOARと統合してアナリストの単純作業をなくし、インシデントを驚異的なスピードで解決して、その対応を数分(または数時間)からわずか数秒に短縮することが求められています。SOARツールを使用すれば、異なるツールからインテリジェンスを収集して統合し、アラートのデータをエンリッチして、1つの画面にまとめて表示できます。

データ収集のプロセスを自動化することで、アナリストはアラートを受け取ると同時に、重要な関連情報を確認することができます。

結論として、オーケストレーションと自動化は、セキュリティアラートの調査と対応を大幅に迅速化できるだけでなく、異なるソースからデータを収集して統合し、アラートをエンリッチすることもできます。判定とアクションをオーケストレーションし、大量アラートの調査、トリアージ、対応を迅速化することで、セキュリティチームはリスクレベルをすばやく判断して適切な対策を講じることができます。

05

内部不正、内部脅威の特定と対応が容易になる

内部不正や内部脅威は特定が難しい一方、その被害は大きくなりがちであるため、UEBA(ユーザーとエンティティの行動分析)は、資格情報を盗み出す、不正を働くといった悪質な行為の兆候を示す不審な行動パターンを検出するための極めて重要なツールといえます。UEBAでは基本的に、機械学習と分析を活用し、データを基に一連のアルゴリズムを実行して、ユーザー規範から逸脱する行動を検出します。これにより、攻撃者が企業の環境内を探り始めるとその行動を特定、追跡します。

従来、UEBAは段階的なアプローチで採用されており、組織は最初に中心となるSIEMを導入してから、UEBAやSOAR(あるいは他のツール)へと拡張していました。しかし現在、UEBAはガートナー社により主要な機能と見なされており、(できれば可能な限りシームレスに)SIEMソリューションと連携することで、ネットワーク内の行動パターンに関するインサイトを提供します。

2つのテクノロジーを1つのプラットフォームに統合することによって、組織は人間の行動と機械の動作の両方を調査して脅威を検出できるというメリットが得られます。また、UEBAをSIEMの一部として組み込むことで、異常行動を認識する精度が上がり、既知と未知の脅威に関する追加のコンテキストを取得できるようになります。これにより、誤検知を減らし、通常のルールベースの相関付けでは検出できない精度の高い脅威を検出できるため、アナリストの作業時間を節約し、チームの作業効率を向上させることができます。

SIEMの動向に関する詳細なインサイトと、セキュリティリーダーのベストプラクティスについては、**ガートナー社の2021年度マジック・クアドラント**をご覧ください。

レポートをダウンロード

splunk>
turn data into doing®

22-22392-Splunk-Top 5 SIEM Trends to Watch in 2022-LS-JA-202204