IBM Security

SIEMに関する6つの誤解

IBM

SIEMに関する6つの誤解の詳細

最近、SIEMソリューションについて調査しましたか?
状況は変わってきています。

SIEMソリューションは扱いにくく、複雑であるため、大企業にしか使えないと誤解されています。確かに、いくつかのSIEMは企業専用のバケットになっていますが、この考えはあらゆる規模の事業向けに設計された、さらに進んだSIEMソリューションを見落としています。

サイバー・セキュリティー業界が大幅なスキル不足に直面していることは、周知の事実です。セキュリティーでもそれ以外でも、ソリューションは、リソースが限られていても仕事で使用が可能になるように設計する必要があります。(おそらく現在あなたはそんな問題を抱えているでしょう)

SIEMに関する 6 つの誤解を検証し、今日SIEMに期待すべきことを調査します。

誤解#1

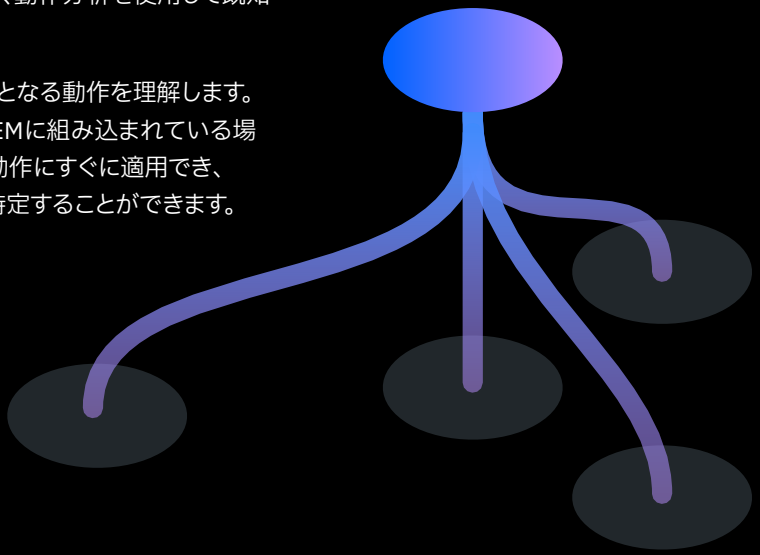
SIEMは既知の脅威のみを検出することができます。未知の脅威には役立ちません。

SIEMソリューションは相関関係のみを利用して脅威を検出し、効果的な相関規則を導き出すので、最初に何を探しているのかを知る必要があります。

真実

効果的なSIEMはリアルタイムの相関、異常検出、機械学習、動作分析を使用して既知および未知の脅威の両方を検出します。

また、高度な相関を利用してドットを結合し、関連した脅威となる動作を理解します。高度な分析およびリアルタイムの相関の組み合わせがSIEMに組み込まれている場合、ネットワーク、アセット、ユーザー、アプリケーションの動作にすぐに適用でき、既知の脅威だけでなく、未知の脅威を示す異常な動作も特定することができます。



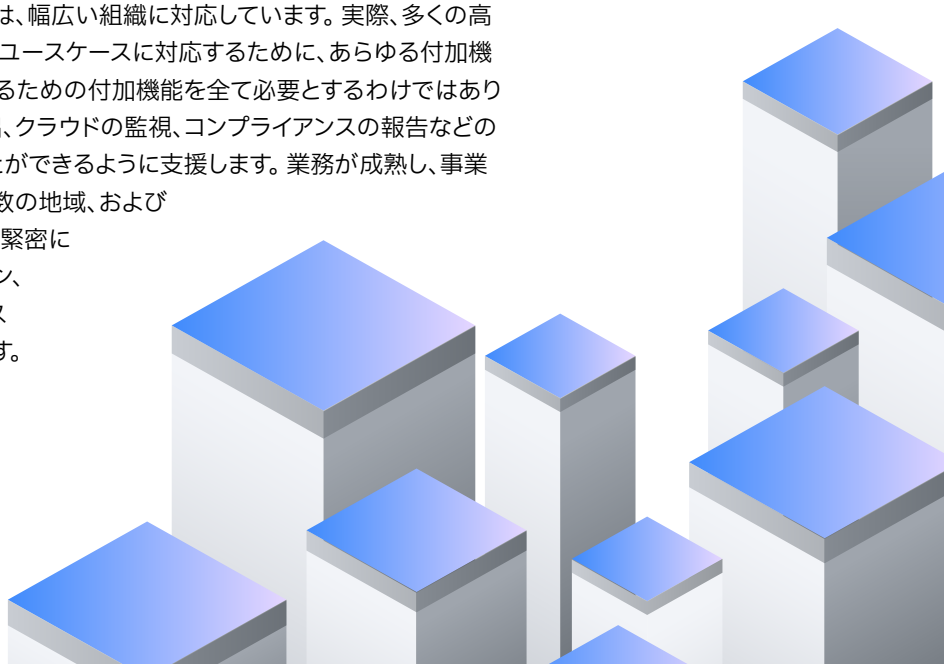
誤解#2

SIEMは高度なセキュリティー・チームを擁する大企業向けです。

定説によれば、市場での最高のSIEMソリューションはかなり大規模な組織に対応できるように調整されるため、主に大規模な組織のみを対象としています。

真実

セキュリティー監視を始めたばかりの成長事業から、高度なユースケースが必要なFortune 20グローバル企業まで、最高のSIEMソリューションは、幅広い組織に対応しています。実際、多くの高度なセキュリティー・チームは、高度で専門的なユースケースに対応するために、あらゆる付加機能を求めますが、優れたSIEMは、価値を提供するための付加機能を全て必要とするわけではありません。理想的なソリューションは、脅威の検出、クラウドの監視、コンプライアンスの報告などの標準的なユースケースを、すぐに使い始めることができるように支援します。業務が成熟し、事業が成長するにつれ、SIEMはより多くの環境、複数の地域、およびディープ・パケット・インスペクション、DNS分析、緊密に統合されたセキュリティー・オーケストレーション、自動化、応答（SOAR）などの高度なユースケースをサポートできるように拡張する必要があります。



誤解#3

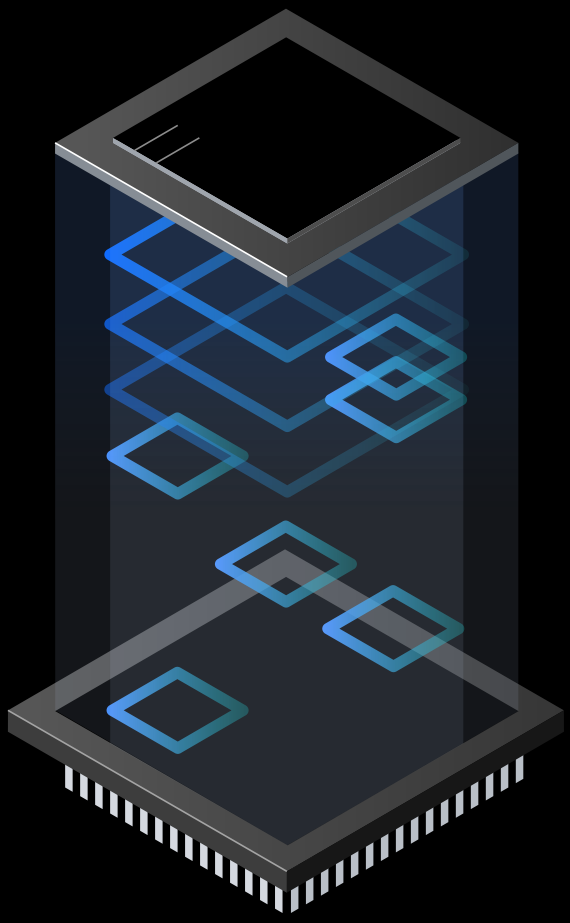
SIEMは大量のデータを必要とするため、そのデータをすべて収集するには非常に高いコストがかかります。

ベンダーによっては、すぐに法外な価格になることで知られていることもあるため、セキュリティー・チームの中には、すべてのSIEMがそうであると思い込んでいる人もいます。

真実

保存されたデータ量に基づいて課金するベンダーを検討している場合、すぐに非常に高額になる可能性があります。しかし、ベンダーによってそのソリューションの価格は異なっています。

何かを約束する前に、どんな問題を解決しようとしているのかを考えてみてください。お客様は小売業者で、支払いカード情報を保護する必要がありますか? Amazon Web Servicesに移行して、新しい環境を可視化する必要がありますか? セキュリティーのために収集するデータは、お客様独自のユースケースに対処するために役立ちます。すべてを分析する必要がない場合は、分析することに振り回されないでください。しかし、規制や組織の方針によってデータ保持の必要もある場合、SIEMベンダーは、ストレージ、検索、レポート作成のみを低コストで提供できます。組織にとって重要なことだけを分析し、残りのログやイベント・データを低コストのストレージに送信することで、SIEMプロジェクトに予算を全て注ぎ込まずにすみます。



誤解#4

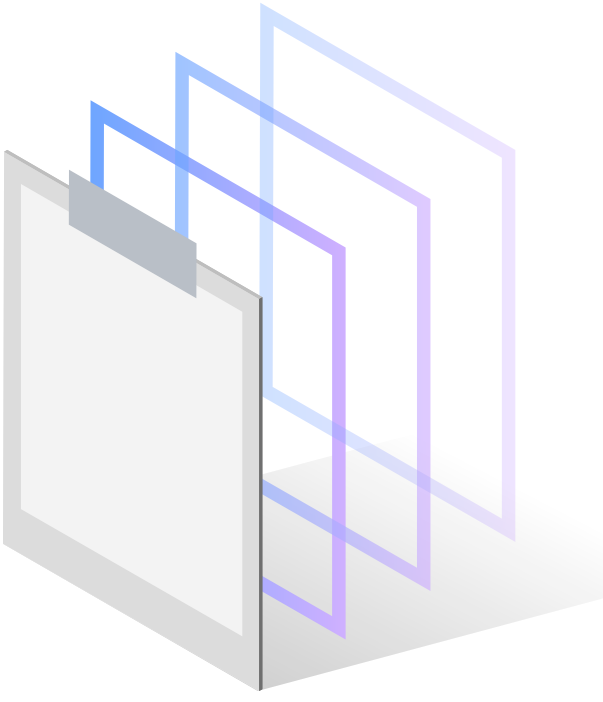
SIEMを効果的にするためには、専任のデータ・サイエンティスト・チームが必要です。

SIEMを効果的にするには、すべての規則と分析をゼロから構築する専任のデータ・サイエンティスト（もしくはチーム）が必要だと言われています。

真実

セキュリティーの知識が豊富なデータ・サイエンティスト・チームが見つからない（あるいは見つけたくない）場合は、あらかじめパッケージ化されたコンテンツを提供するベンダーを探すとよいでしょう。

ベンダーによっては、「どうせソリューションはカスタマイズするのだから、白紙から始めよう」というアプローチを取る場合もあります。実際のところ、現在のセキュリティー・チームは、このような専門的なスキルを必要とする大規模プロジェクトを引き受けるだけのリソースを持ち合わせていないのが現状です。どのようなSIEMソリューションでも、ネットワークに関する情報を提供する必要がありますが、それが終わると、事前に導き出された規則、分析、相関ポリシーを利用して、すぐに脅威の検出を開始できます。全く白紙の状態から始める必要はありません。それでも心配な場合は、多くのSIEMベンダーがマネージド・セキュリティー・サービス・プロバイダー（MSSP）と提携しているので、先進的なSIEMのメリットに加えて、セキュリティー運用の専門家にサポートしてもらうというメリットもあります。



誤解#5

ログ管理スタックでSIEMと同等の可視性を実現できます。

ログ管理およびデータレイク・ベンダーのクリエイティブなマーケティングにより、ログ管理ソリューションが、脅威の発見と調査においてSIEMよりも優れていると思われることがあります。

真実

ログ管理ツールは、コンプライアンスや監査のユースケースを達成できますが、リアルタイムの分析やアラートには不十分です。

ログ管理は、過去10年来の問題に対するソリューションでした。企業は、サーベンス・オクスリー法（SOX）、ペイメント・カード業界（PCI）などの業界規制に対する監査基準を満たすためのソリューションを必要としていたのです。ログ管理スタックは、ペタ・バイト規模の検索とインデックス作成ができるということで近年復活を遂げましたが、リアルタイム分析の欠如によって、クエリー、ピボット、脅威の探索など、手動での検出の責任は、すでに限られたスタッフしか負えません。

ほとんどのSIEMプロバイダーは、集計、解析、保存のためのログ管理レイヤーまたはデータレイクをソリューションの一部として提供しています。多くの場合、ログ管理レイヤーはSIEMとは別に認可されるため、費用対効果が高く予測可能なホストベースの価格モデルでセキュリティー・データレイクを確立することができます。SIEMの付加価値は、監視と検出のための困難な作業を行う、すぐに使える分析（リアルタイム相関、機械学習など）にあります。簡単に言うと、ログ管理はSIEMそのものではなく、SIEMの機能の一つです。

誤解#6

SIEMは、現在の環境では他のソリューションとの統合が困難です。

SIEMは、他のソリューションからのデータに依存して価値を提供しているにもかかわらず、他のソリューションとの統合が困難であるという評判があります。

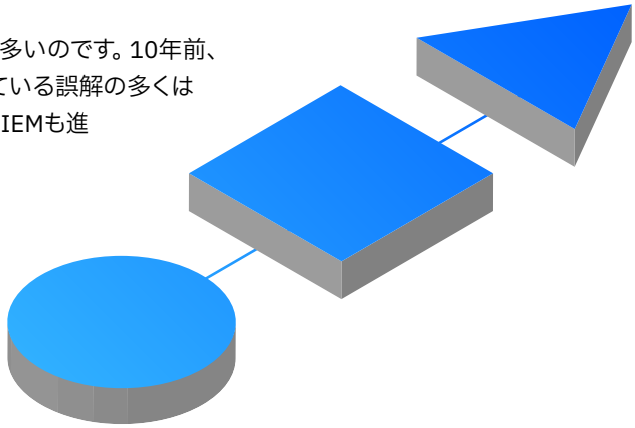
真実

主要なSIEMソリューションは、統合が容易でなければなりませんが、幸い、多くのソリューションは容易に統合できます。

10年前に市場に登場した初期のSIEMは、ニーズの変化やテクノロジーの進化についていけず、統合が困難でした。しかし、そのような企業は完全に消滅したか、大きく苦戦しているのが現状です。今日の主要なソリューションは、市販のITおよびOTとすぐに統合できる数百もの機能を備え、カスタム・アプリケーションとの統合やログ解析のためのシンプルなコネクターを提供しています。どのような統合機能があり、ベンダーが完全に対応しているかご興味をお持ちの場合は、各ベンダーのカスタマー・サポート・サイトやApp Exchangeを参照してください。

現在の固定観念は、時代遅れのテクノロジーに惑わされたものであることが多いのです。10年前、あるいは5年前にSIEMソリューションを評価した場合、現在最も広く流布している誤解の多くは真実でした。しかし、テクノロジーと脅威の分野が進化したのと同じように、SIEMも進化しています。

脅威の検出やログ・マネージャーのログを理解するのに苦労しておられるなら、今日こそSIEMソリューションをもう一度見直して、その変化をご自分で発見する日かもしれません。



IBM Security QRadarについて

IBM Security QRadarは、企業全体のセキュリティー・データを一元的に可視化し、最も優先度の高い脅威に対して実用的な見通しを提供する柔軟なソリューションです。このソリューションはQRadar SIEMをベースとしており、何百もの事前定義された規則と分析機能、およびIBM X-Forceの脅威インテリジェンスが含まれています。すぐに使える、500以上の統合機能と160以上のアプリケーションにより、お客様は迅速に運用を開始し、新しいセキュリティーとコンプライアンスのユースケースを容易に追加することができます。ログ・ストレージ、ユーザー行動分析、ネットワーク・パケット・インスペクション、脆弱性管理、AIを活用した脅威調査などのオプションの完全統合コンポーネントは、単一のインターフェースから容易に追加・管理でき、あらゆる規模のお客様が、ニーズの変化に応じて容易に拡張・縮小することが可能です。

詳細は www.ibm.com/jp-ja/qradarでご確認ください。

IBM Security

日本アイ･ビー･エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21

IBM