elastic

SIEMの運用バリューを向上させる

elastic.co/jp →

目次

はじめに

市場の変化に対応するためにデジタルトランスフォーメーションに取り組む多くの組織が、セキュリティアプローチの再評価を迫られています。新しいWeb製品やWebサービス、モバイルアプリが登場し、リモートワークをサポートする必要も生まれたことで、新しいタイプのサイバー攻撃が増加しています。**これらの攻撃に対処するために、セキュリティチームは遅れを取らないよう速やかに進化する必要があります。**

そのためには、非効率な運用を避けることが重要です。セキュリティチームが最善を尽くしても、運用面で非効率な部分があればビジネスの妨げとなる場合があります。SaaSの爆発的な普及、現行のプライバシー関連法令、セキュリティ機能の統合を求める指示への対応により、運用の複雑さは増す一方です。

効率を維持しながら運用をコントロールするための最初のカギは、組織のセキュリティ情報およびイベント管理（SIEM）プラットフォームでデータをすぐに利用できるようにすることにあります。クラウド、モノのインターネット（IoT）、モバイルソース、オブザーバビリティデータなど、セキュリティチームが必要とするデータの量と種類は爆発的に増加しています。その結果、ビジネスの保護に必要なインサイトを得るのに欠かせないイベントアクティビティも大幅に増加しています。

このようなデータの爆発的増加に伴い、SIEMの制限事項から運用上の課題が生じることも少なくありません。新たな課題に対応するためには、**SIEMのアプローチを見直す時期に来ている**のかもしれません。

175 ZB

IDCは、2025年までに世界のデータは175ゼタバイトに増加すると予測

416億台

2025年までに416億台のコネクテッドデバイスが79.4ゼタバイトのデータを生成する見込み

420億ドル

PwC社によるGlobal Economic Crime and Fraud Survey2020調査の回答者は、不正行為による損失総額が420億ドルに上ったと回答

セキュリティ要件の変化

組織が採用するビジネスモデルにおいてクラウド中心の傾向が高まるにつれ、セキュリティチームは、組織の最も貴重な資産であるユーザー、アプリケーション、エンドポイント、データを確実に保護する責任をより強く求められるようになりました。一方で、下記に挙げたような状況によって、セキュリティチームによるKPIやメトリックの達成は難しくなっています。

人材

新たな攻撃手法や高度化する攻撃手法に遅れをとらないことは必須の課題です。

- セキュリティスキルが不足している
- 負担を抱えているセキュリティチームが、協力体制の向上や作業の迅速化、効率化に取り組んでいる

プロセス

クラウドイニシアチブが急増する中、運用効率とスピードを維持する必要性が高まっています。

- 大量のデータがクラウドに移されつつある
- リモートワーカーやパートナーがサポートを求めるクラウドソリューションが増えている

テクノロジー

検知回避アクティビティを可視化したり、脅威にコンテキストを付加するために必要な詳細情報を得たりするには、大規模なデータソースに対するサポートが不可欠です。

- オンプレミスとクラウド全体を対象に応答性の高いクエリや分析を実行することが困難
- 多くのシステムで、大規模なデータソースへのアクセスがコスト高になる場合がある

セキュリティチームは、デジタルトランスフォーメーションによって攻撃面が増えることを痛感しています。コネクテッドデバイスやクラウドサービスが増えるたびに、攻撃者に悪用される可能性のある新たなベクトルが生まれ、重大なセキュリティ脅威や資産の露出によってビジネスリスクが増大するおそれがあるためです。**この状況に対する最も肝要な要件は、的確な意思決定を迅速に下せるように、適切なタイミングで適切なコンテキストを把握することです。**

データをフレームワークとして活用し、セキュリティ戦略を見直す

変化と拡大を続ける攻撃面を絶えず把握しようとするのは、あまり現実的とは言えません。インジェスト単位やイベント単位のライセンスモデルや、クラウドのスケール要件を満たしていないアーキテクチャーでは、妥協を強いられることもあります。セキュリティチームは、日々の運用で対象とするデータと除外するデータを決定するのに時間とリソースを費やすことが多いため、SIEMでの可視性が制限されたままになり、データサイロ、チーム間のサイロ、プロセスのサイロといった運用上のサイロが発生することがよくあります。

セキュリティチームは、大規模なデータソースや履歴データなど、SIEMの対象とすることが困難なデータを保持するために妥協やその場限りのアプローチを行うのではなく、データのニーズを中心に据えた別のアプローチを採用するようになってきています。最新のSIEMの基盤は、セキュリティチームがサイロを解消できるように、あらゆるデータに対応していることが求められています。

最新のSIEMを使用すれば、セキュリティチームは多層的なエコシステム全体を対象に、従来型のデータソース、非従来型のデータソース、大規模なデータソースなど、あらゆる種類の膨大なデータを迅速かつ正確に検索できます。このような基盤を整えることで、監視とコンプライアンス、脅威検知と防御、ハンティングとインシデントレスポンスなど、**あらゆるセキュリティユースケースを大規模に運用**しながら、不正行為、プライバシー侵害といったビジネスを危険にさらす優先課題にも対応できるという大きなメリットを得ることができます。重要なのは、**一元的なアプローチでセキュリティインサイトを収集、分析、可視化し、それに対応**する能力をセキュリティ運用チームが獲得することです。

一元的なアプローチがSOCにもたらすメリット

一元的なアプローチは、セキュリティチームに多くのメリットをもたらします。強力なデータセキュリティ、データ処理、データ可視化の機能を備えた単一のデータストアは、分散環境において必要なコンテキストを提供し、あらゆるデータから価値あるセキュリティインサイトを引き出します。高精度の検知、検証済みの機械学習ジョブ、オンプレミスとクラウドに対応したすぐに使える手法など、適切なセキュリティ分析機能があれば、セキュリティチームは、セキュリティ態勢の改善、既知と未知の脅威の検知、迅速な対応による被害の回避と将来のインシデントの防止を実現できます。戦略面でも、**大きな変化が生じたときに、迅速な進化を達成できます。**担当者は、次のような活動をする中で、幅広いスキルセットを身に付けることができます。

より多くのコンテキストを活用してデータをより適切に操作し、ノウハウを分析

協力して新しい調査を探し、新しい検知を実装

新しい可視化と運用手順を開発

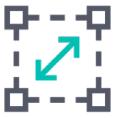
脅威アクターをプロファイルし、敵対的な振る舞いを模倣

多くのチームがハンティングを担当できるようになるほか、プラットフォームレベルの強力な統合機能により、新しい種類の脅威や新たな規制への対応を簡素化する、非常に効率的な手順を実現できます。

一元的なアプローチを導入することで、SOCは、脅威ハンティング、SIEM、脅威調査、コンプライアンス、セキュリティ監視および調査、デジタルフォレンジックとインシデントレスポンス、エンドポイント保護、不正防止など、多くのセキュリティ機能に関する複雑なセキュリティ問題を解決できます。

包括的な可視性

セキュリティインサイトを収集し、ビジネスの目標に沿った成果を得るために必要なあらゆるデータソースを取り込むことができます。



クラウドスケーラビリティ

数年にわたる履歴データコンテキストも含め、脅威を検証するために必要なコンテキストを組織全体から取得できます。

SOCの効率向上

優先度の高い問題を迅速に発見し、他のツールやテクノロジーと簡単に統合して迅速な調査や対応を実現します。

セキュリティチーム全体にとっての価値

セキュリティエンジニアと管理者

- データソースの種類にかかわらず、環境全体のログ、フロー、コンテキストデータを一元的に分析
- 複雑な分散環境にすばやくアクセスして検索できる高速で横断的な検索
- 多額のコストをかけずに大規模なデータソースをインデックスし、簡単にアクセス

セキュリティアナリスト

- 複雑な脅威をより早く検知できる精度
- 対応を加速し、効率を向上できるスピード
- 脅威検知を自動実行し、MTTDを最小化

SOCマネージャー

- 環境全体で高いアウェアネスを維持し、セキュリティ態勢を向上
- 未知の問題を特定しながら、既知の問題の再発を回避
- 高いコストをかけずにセキュリティKPIを達成

elastic

SIEMがビジネスの足かせになっていませんか？

今日、セキュリティ関連のデータは、クラウドサービス、ネットワークおよびユーザーアクティビティ、エンドポイント、アプリケーション、コネクテッドデバイスなど、多くのソースから取得できます。これらのデータソースのすべてにアクセスするSIEMソリューションの多くでは、分析時間がコーヒー休憩を取れるほど長くなったり、デプロイコストが高くなったりします。

SIEMの中には、機械学習用やイベントベースの相関関係用など、複数のタイプのセキュリティ分析用に別々のデータストアを使用して構築されているものもあり、脅威ハンティングのコンテキストやフォレンジックエビデンスなどのために、さらに別のデータストアにデータをアーカイブしなければならないこともあります。前述したように、このようなサイロは、コンテキストの共有、共同作業、ケース管理、脅威への対応が非効率になる原因になります。

SIEMはSOCの迅速な進化に貢献するはずですが、多くのSIEM製品は、セキュリティチームがデータサイロやタスクサイロを解消するのに役立つスケールや柔軟性を備えていないため、調査ワークフローがサイロによって制限されることになります。その結果、運用面でもサイロが発生し、セキュリティチームの迅速かつスマートで効率的な活動が妨げられてしまいます。

従来のSIEMソリューションは、運用効率の面で次のような共通の課題を抱えています。

- セキュリティデータのソースが統合されておらず、企業内のさまざまなデータストアに存在するため、全体像を把握することが困難である。
- データ保持期間が短すぎるため、検知、調査のコンテキスト、脅威ハンティングについて妥協せざるを得ない。ドゥエルタイムの長い攻撃について、侵害の範囲を特定することが困難である。
- 高度で永続的な脅威ではないもののビジネスにとって非常に現実的な脅威であるアクティビティに関するコンテキストを得るために必要な適切なデータソースをセキュリティアナリストが確保していない。
- モデルを開発するデータサイエンティストとコンテキストを解釈する熟練した脅威ハンターが社内にいないと、SOCチームが機械学習ツールを活用できない。
- セキュリティエンジニアが、データの正規化プロジェクトに膨大な投資を行ったり、コンテキストリッチな新しいデータソース（大容量データなど）を追加する必要があるときにSIEMの基盤となるデータファブリックを常に再構築したりしなければならない。データをすでに「知っている」必要がある。
- 調査チームは膨大な時間を費やしてSIEMルールを開発しているが、このルールは脆弱で回避技術に対して弱く、適切なデータから得られる高精度のコンテキストも不足している。
- ティア1やティア2のアナリストがアラートの追跡に多くの時間を費やしているが、成果を得られなかったり、他のデータストアから追加のコンテキストを取得する必要が生じたりして、遅延や非効率が発生している。
- 開発者が、統合のトラブルシューティングやベンダーのアップデートへの対応にほとんどの時間を費やしている。

最新のSIEMで保護を強化

最新のSIEMは、規模、スケール、場所の制約を受けることなく、すべてのセキュリティデータにアクセスできます。セキュリティチームは、環境全体を可視化することで、脅威をより効率的に検知して迅速に対応するために必要な、豊富なコンテキストと履歴のルックバック期間にアクセスし、脅威の優先順位をより正確に決定できます。

あらゆるデータにアクセス

リアルタイムなインサイトと履歴情報

SOCの業務スピードを最大化

ElasticセキュリティをSIEMとして使用して運用効率を向上

セキュリティチームが管理するデータは増加する一方で、チームはそのすべてを迅速かつ正確に検索、分析、自動検知できなければなりません。最新の脅威に対応するには、従来のセキュリティデータ、クラウドインフラ、アプリケーションデータ、数年分の履歴データを使用して、効果的な調査、ハンティング、脅威のプロファイリングなどを行うために、瞬時に相関付けできる必要があります。

セキュリティチームはElasticセキュリティを使用することで、統合されたデータにアクセスしたり、脅威とビジネスのコンテキストを使用して調査結果にコンテキストを付加したり、履歴データを使用して最適な解決策を迅速に発見したりできます。Elasticセキュリティは、SIEM、エンドポイントセキュリティ、脅威ハンティング、クラウド監視、不正検知など、多くのユースケースに対応しているため、SOCは検索と可視化の力を活用して、一元的なアプローチで脅威の検知、防止、対応を行い、組織を保護できます。

Elasticセキュリティで作業をスマートに

包括的な可視性を実現

Elastic Common Schemaで正規化したデータをBeatsで収集し、セキュリティ関連のデータをすべてインデックスして、組織全体のデータサイロを解消します。Kibana、Lens、Canvasを使用すると、直感的ですぐに使えるダッシュボードや、ニーズに合わせてドラッグ&ドロップでカスタムビジュアライゼーションを作成できます。

セキュリティインサイトをすばやく獲得

schema on writeとschema on readの両方のフォーマットを使用してデータを取り込むことで、最適なクエリパフォーマンスを実現し、取り込み後のフィールドの追加や変更も柔軟に行えます。Elastic Stackが誇るスピードで、数秒でダッシュボードに結果を表示します。優先順位付けされた相関関係でアラート疲れを解消します。

数年分の履歴データを取り込み

検索可能スナップショットを活用することで、検知、調査コンテキスト、脅威ハンティング、クラウド監視などに必要なセキュリティデータにコスト効率よくアクセスできます。ドゥエルタイムが数か月から数年にわたる侵害の範囲を特定できます。

ドゥエルタイムの短縮

Elastic社内のセキュリティ調査チームによって開発された、MITREマッピングを使用した設定不要の検知機能による自動検知と、パワフルで直感的なEvent Query Language（EQL）を活用したカスタム検知により、高度な脅威のツール、戦術、手順を検知する相関付けを実行できます。

悪意のある異常なアクティビティを発見

タイムスタンプ付きのデータソースに教師なし機械学習ジョブを適用し、潜在的な脅威を構成する単独の異常や関連する異常を特定します。教師ありと教師なしの機械学習を組み合わせて、ドメイン生成アルゴリズム（DGA）などの手法を低い誤検知率で検知します。

セキュリティ運用ワークフローを最適化

Elasticセキュリティのインタラクティブなワークスペースを使用して、脅威の検知と対応、イベントのトリアージ、エビデンスの収集をインタラクティブで直感的なタイムライン上で行うことができます。組み込みのケース管理機能や、主要なSOAR（セキュリティオーケストレーション、オートメーション、レスポンス）およびワークフローベンダーとの統合を活用し、対応と復旧を迅速化できます。

最先端のSOCを構築

Elasticセキュリティは、あらゆる場所で最新のセキュリティチームの技術基盤として機能しています。オープンなプラットフォームによるElasticのセキュリティアプローチは、容易な統合、高い柔軟性、コミュニティ主導のコントリビューションやコラボレーションを実現し、SOCチームの迅速な進化と意思決定の向上と迅速化を支援します。

まとめ

セキュリティチームは、拡大し続けるセキュリティ環境で組織を守りながらも、運用効率を維持する必要性を見失うことがあってはなりません。ElasticセキュリティをSIEMとしてデプロイすることで、セキュリティに関連するすべてのデータへのアクセスや、履歴データへのコスト効率のよいアクセスが可能になるため、より多くのユースケースに対応して、SIEM環境の運用価値を全体的に高めることができます。先進的な**セキュリティチームがElasticセキュリティをSIEMとして選択しているのは、一元的な検知、予防、対応アプローチが必要だからです。**

Elasticは環境全体にわたる包括的な可視性を提供し、問題の特定や解決のスピードと効率を高めます。また、ハイブリッド環境全体にクラウドスケーラビリティを提供し、現在のチームの分散状況や運用上のサイロの数にかかわらず、SOCが効率を最大化できるよう支援します。ElasticセキュリティによるSIEMへの新しいアプローチでビジネスを保護してみませんか。

ぜひ実際にElasticセキュリティに触れてください。

Elasticセキュリティが搭載されたElastic Cloudをお試しください（14日間無料、クレジットカード不要）。オンプレミス版も、無料でデプロイが可能です。

Elasticセキュリティを無料で試す ⟶

elastic

Search. Observe. Protect.

Elasticのテクノロジーはデータを大規模かつリアルタイムに処理し、エンタープライズサーチ、オブザーバビリティ、セキュリティに活用します。ドキュメント検索からインフラの監視、脅威ハンティングまで対応するElasticのソリューションのベースは、あらゆる環境にデプロイでき、あらゆるタイプのデータから瞬時に実践的なインサイトを抽出する単一の、無料かつオープンなテクノロジースタックです。Elastic StackはCisco、Goldman Sachs、Microsoft、The Mayo Clinic、NASA、The New York Times、Wikipedia、Verizonを含む世界中の企業や組織で採用され、ミッションクリティカルなシステムを支えています。Elasticは2012年に設立され、ESTCのシンボルでNYSEに株式を公開しています。詳しくは、elastic.co/jpをご覧ください。

米国本社
800 West El Camino Real, Suite 350, Mountain View, California 94040
代表 +1 650 458 2620、セールス +1 650 458 2625

info@elastic.co