sysdig

概説 : BUSINESS VALUE BRIEF

クラウド攻撃への調査能力を強化し、ビジネス価値を高めよう

現在のクラウド攻撃は、迅速かつ巧妙になっています。脅威アクターは自動化を武器に攻撃を加速させつつ、クラウドのアカウントやワークロード間をすばやく移動しています。このような攻撃を阻止するためには、時間が最も重要な要素となります。つまり、侵害が長引けば長引くほど、攻撃者はより多くのデータを流出させることが可能となり、同時に企業や組織はより多くのコストを被ることになります。攻撃者が脆弱性の悪用方法を特定してから攻撃を実行するまでに必要となる時間は10分もかかりません。このため、クラウド調査を迅速に行う力の確保が不可欠です。

一方、ほとんどのクラウド調査は、効果的な対応を可能にするには時間がかかりすぎます。従来のEDR（Endpoint Detection and Response）ツールは、可視性のギャップをもたらすほか、クラウド環境で何が発生したかを迅速に理解するために必要となるコンテキストを提供しません。完全な可視性なしでは、セキュリティチームは、攻撃者の行動の一部しか見ることができない不完全な調査しか行えないのです。また、データがサイロ化されているため、アナリストは複数のツールやドメインにまたがるエビデンスを手作業で収集して相互に関連付けしなくてはならず、その結果、修正作業に大幅な時間がかかっています。セキュリティチームには、複数のクラウドドメインにまたがる調査結果を関連付けることができるような、クラウドネイティブ環境向けに設計されたツールが 必要です。

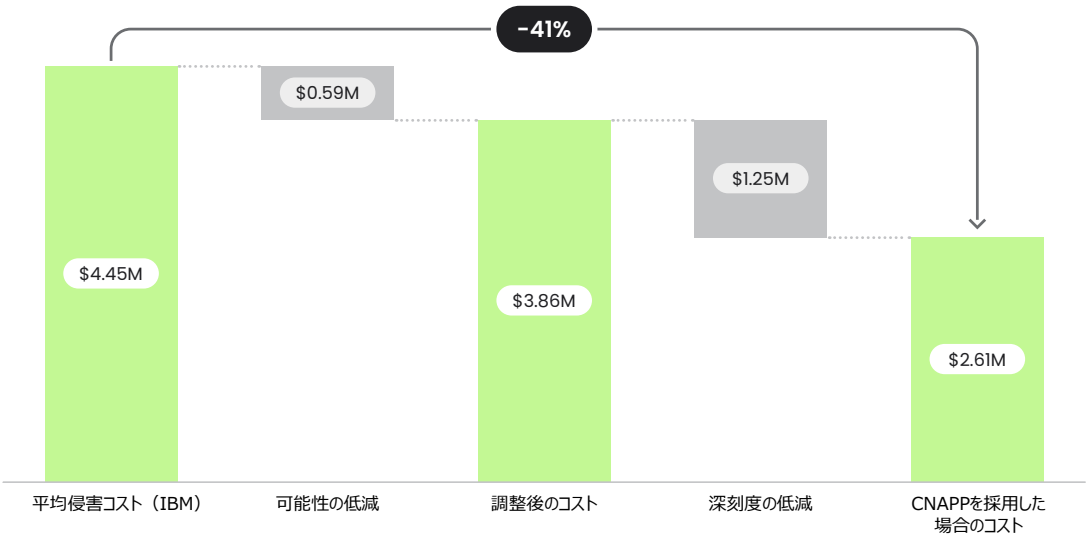
この文書では、Sysdigが提供する強化されたクラウド調査を紹介します。そして、ビジネス価値を創造し、侵害コストを削減する方法を見出していただけるでしょう。 また、インサイトの迅速な相互関連付けを行い、重要なコンテキストを明るみに出すことで、セキュリティチームが、適切な情報に基づいた、より迅速な意思決定を行える方法についても紹介します。

クラウド検知と対応により インシデントコストを最小化

リアルタイム検知とクラウドネイティブなコンテキストにより迅速な調査が可能となります。これにより、アナリストの時間を節約するだけでなく、インシデントのコストも削減します。攻撃が完全に実行される前にセキュリティチームが調査して対応できれば、インシデントが侵害へと発展するのを防ぐことができるほか、関連コストを最小限に抑えたり、一掃することも可能です。また、効率的な調査は、インシデントを抑制し、侵害リスクを低減するための鍵となります。インシデントが組織の機密データにとっての脅威となるのを防ぐには、時間が最も重要な要素です。なぜなら、侵害されている期間は、その深刻度とコストに直結するからです。データ侵害の世界的な平均コストは**445万ドル**であり[1]、Sysdigの脅威リサーチチームの調査では、攻撃が対処されないままの状態になっているために、被害額が毎日数万ドル増加している事例があることが明らかになっています。

インシデント対応は「総動員」で対応するような状況にもなり得ます。すなわち、場合によっては、セキュリティ専門家だけでなく、開発者、ネットワークエンジニア、アーキテクト、そして経営幹部をも巻き込む必要があります。このような「戦争時の作戦指令室」のような状況には、関与する役職やその頻度にもよりますが、年間数万ドルから数10万ドルのコストがかかる可能性があります。EDRのような従来のソリューションには、複数のドメインやツールを相互に関連付ける機能がないため、そのギャップを埋めるために、ますます多くの人員が必要となります。

クラウドの検知と対応における555ベンチマークとは、「5秒で検知・5分でトリアージ・5分で対応」を意味するものであり、これは最新の攻撃に関する現実を認識することを企業や組織に課すものです。Sysdigでは、555ベンチマークを満たす効果的なクラウドの検知と対応（CDR）ソリューションを導入することで　侵害の可能性を減らし、エスカレートした脅威の深刻度を抑えることにより、**侵害リスクを41% 低減し、コストを180万ドル節約できる**可能性があると試算しています[2]（下図参照）。



Sysdigの導入で、侵害リスクを41%削減し、コストを180万ドル節約できる可能性がある（平均侵害コストを445万ドルと想定）

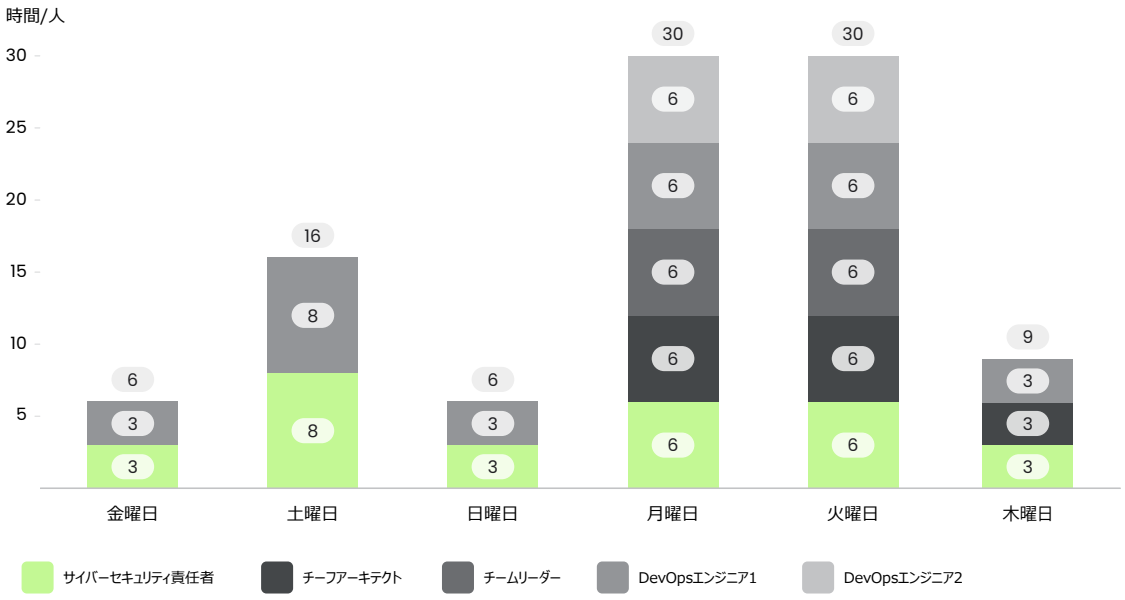
1　IBM Cost of a Data Breach Report 2023
2　『IBM Cost of a Data Breach Report 2023』に示されていた平均データ侵害コスト445万ドルに基づいて計算

Sysdigは、高度な検知機能と包括的なクラウドネイティブコンテキストを統合することで、これを実現します。Sysdigのプラットフォームは、複数の環境における、リソース、イベント、アイデンティティ、ポスチャー、脆弱性データ間の相互関連付けを自動化することで、調査を合理化します。これにより、調査結果の収集と関連付けの手作業が不要になるため、セキュリティチームの貴重な時間を節約できるほか、調査の有効性を高め、最終的にインシデントコストを削減できるようになります。

効果的なCDRソリューションを導入すると、侵害リスクを41%削減し、コストを180万ドル節約できる可能性があります。

従来の調査ツールによる生産性の損失

従来の調査ツールを使用した場合、ある金融サービス会社では、わずか2件のセキュリティインシデントに1週間のうち97時間を費やしていました。これには、実際のインシデントを調査する時間も含まれていましたが、別のインシデントがリスクに該当しないことを確認するのにもかなりの時間を要していました。これらのインシデントでは、サイバーセキュリティの責任者とチーフアーキテクトを含む5人の担当者の時間を必要としました。市場レートに基づくならば、この金融サービス会社は、これらの2件のインシデントに費やした時間だけで、Sysdigにかかるコストの20%も支払ったことになります。



この金融サービス会社では、わずか2件のインシデントに1週間で97時間を費やした

コンテキストドリブン型の意思決定により ダウンタイムコストを一掃

効果的な意思決定を行うためのデータが不足している場合、セキュリティチームは、侵害の痕跡に直面した際に難しい選択を迫られます。セキュリティチームは、貴重な資産やデータを保護するために、重要な本番システムをオフラインにするなど、即座に軽減策を講じることもできます。しかし、これは大きなダウンタイムとコストにつながりかねません。1時間のダウンタイムが組織にもたらすコストは、**通常145,000ドルから450,000ドルの間**の金額となります。このように企業や組織は、莫大な経済的打撃を受ける可能性があるため、意思決定を慎重に検討することが極めて重要となります。

その一方で、侵害は企業に数100万ドルの損害を与えるため、システムをオフラインにすることに遅れると、コストが飛躍的に増大する可能性があります。攻撃者は、より複雑で有害な活動から注意をそらすために、クリプトマイナーの導入のような、より単純な攻撃をよく使用します。これはSCARLETEEL攻撃における重要な戦術であり、攻撃者は、被害者の注意をそらすためにクリプトマイニングを使用することで、認証情報を見つけ、プロプライエタリなソフトウェアを窃取します。

関連データの欠如は、過剰反応と不必要なダウンタイムを招き、侵害コストを**簡単に100万ドル以上**へと引き上げます。このシナリオは、意思決定に情報を提供する正確でリアルタイムのコンテキストの必要性を浮き彫りにしています。EDRのようなレガシーツールは、意味のあるマルチクラウド関連のインサイトとコンテキストを欠いており、クラウド攻撃に関しては不完全なストーリーしか伝えません。セキュリティチームには、攻撃の連鎖を完全に調査し、インシデントの全容を理解する能力が必要です。

Sysdigは、リアルタイムインサイトと自動的なクラウド間のコンテキストと相互関連付けを組み合わることで、セキュリティチームと開発チームがクラウド調査における「5つのW」を理解できるよう支援します。Sysdigの迅速な調査フローを利用することで、チームは、リッチなコンテキストドリブン型の攻撃ストーリーを構築できるほか、脅威アクターがどのような行動を取ったか、どのように環境内を移動したか、を正確に特定できるようになります。さらには、イベントとアイデンティティ間の相互関連付けも正確に解明します。このストーリーを活用することで、組織の運営や財務に損害を与えることなく、脅威を効果的に軽減する方法について、十分な情報に基づいた意思決定を行うことができます。

ダウンタイムが1時間発生すると、**145,000ドルから450,000ドル**のコストを被ることになり、インシデントのコストは簡単に**100万ドル以上**に膨れ上がります。

調査ワークフローの最適化により、将来のインシデントを防御

セキュリティチームは、EDRツールをCDRユースケース用に拡張しようと試みますが、多くの場合、それを他の予防的コントロールと統合できないことに気付きます。セキュリティチームと開発チームは、点と点をつなげようとする際に、基本的に異なる言語を話します。EDRツールは、クラウドインシデントに関する有意義なコンテキストを欠いているため、こうした課題をさらに複雑にしています。この結果、セキュリティチーム、開発者、プラットフォームチーム間の連携不足が常態化するほか、組織的なセキュリティポスチャーが弱体化し、将来のインシデントの防止が困難になります。攻撃が発生すると、これらのチームは協力して、アクセス許可を変更するか、または悪用された脆弱性を修正することにより、攻撃の範囲を軽減しなければなりません。

また、ポストインシデント分析も、将来のインシデントを軽減するために不可欠です。なぜなら、これらの分析は、チームが初期の攻撃ベクターとその後のアクティビティの理解に役立つからです。Mandiant社によると、攻撃の68%は、脆弱性、フィッシング攻撃、または認証情報の窃取から始まっています[3]。このような侵入地点は、将来、効果的に塞ぐことができますが、それが可能となるのは、インシデントにつながるイベントを徹底的に理解している場合に限られます。包括的なポストインシデント分析により、セキュリティチームは攻撃者が利用した弱点を特定し、それに応じて防御を強化できます。これにより、当面の脅威を軽減するだけでなく、同様のインシデントを防御するための貴重なインサイトを得ることができ、最終的には繰り返されるインシデントのコストを削減できます。

Sysdigが提供するこの強化された調査フローは、複数のドメインにまたがるインサイトを組み合わせることで、複数のアナリストが協力して攻撃の軌跡を即座に理解できるようにします。アイデンティティとイベントの一元化、リッチ化、および相互関連付けを行うことで、セキュリティチームとプラットフォームチームはサイロ化を解消し、調査結果を容易に共有して調査を迅速化できるようになります。Sysdigは、これらのチーム間の緊密な協力を促進することで、リアルタイムで脅威に対応し、将来の侵害を防止するための能力を強化します。インシデントがどのように発生したかを迅速に理解することで、侵害の直接的なコストを抑えるだけでなく、同じ弱点が再び悪用されないように保証することで、将来のコストも削減できます。

> 過去には、調査に最長で1週間かかることもありました。しかし、Sysdigを使えば、それは5～10分の作業で済みます。
>
> **セキュリティオペレーションプロバイダーの情報セキュリティ責任者**

3 Mandiant M-Trends 2023 Report

Sysdigについて

クラウドでは、1秒1秒が重要です。攻撃は瞬時に進行します。このような条件の下で、セキュリティチームはビジネスを減速させることなくクラウド環境を保護しなければなりません。Sysdigは、ランタイムインサイトとオープンソースのFalcoを通じて、リスクの変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。また、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を発見し、真のリスクに優先順位を付けます。予防から防御までをサポートすることで、Sysdigは、企業にとって重要なこと、すなわちイノベーションに集中できるよう支援します。

詳細は、sysdig.jpをご覧ください。