sysdig

BUSINESS VALUE BRIEF

クラウドセキュリティにおけるGenAIのビジネス価値

Sysdig Sage™で人による対応を加速

クラウド攻撃は常に進化しており、より高速かつより巧妙になっています。脅威アクターがAIと自動化を武器に攻撃を加速させている今、セキュリティチームは防御を強化して脅威の一歩先を行く必要があります。最新のクラウド環境で時間に追われるセキュリティチームにとって、従来のセキュリティツールやプロセスはますます不十分で非効率的なものとなっています。

サイバーセキュリティにおいても、生成AIは、セキュリティ運用の有効性を高めるために役立つ強力なツールとして登場しています。これまでのところ、AIセキュリティアシスタントは基本的なクエリと要約を提供してきましたが、クラウドへの脅威の全体像をリアルタイムで調査して把握するためには、より多くのことが必要となります。

Sysdig Sageは、Sysdigが開発した生成AIセキュリティアナリストです。Sysdig Sageは単なる情報の要約にとどまらず、インシデントを徹底的に分析し、人による対応を加速化します。本稿では、優れた設計、自律的でかつ包括的なAIセキュリティアナリストが、生産性の向上、侵害がもたらす影響の軽減、セキュリティ運用コストの削減をもたらすことで、ビジネス価値の創出にどう影響を与えるか、を紹介します。

AIによる生産性の向上、エスカレーションとコストの削減

クラウドに投資している企業や組織は、クラウドネイティブアプリケーションを保護することの複雑さに直面しています。リリースの速度と量がクラウド攻撃のスピードと組み合わさることで、すでに負担を抱えているセキュリティチームに、さらに追い打ちをかけています。さらに悪いことに、クラウドセキュリティに関する専門知識の不足に悩まされているとも報告されています。

ESGによると、スキルギャップに加えて、変化、複雑性、アラートの量、可視性のギャップといった複数の要因が、セキュリティ運用チームの主要な課題として報告されているとのことです。

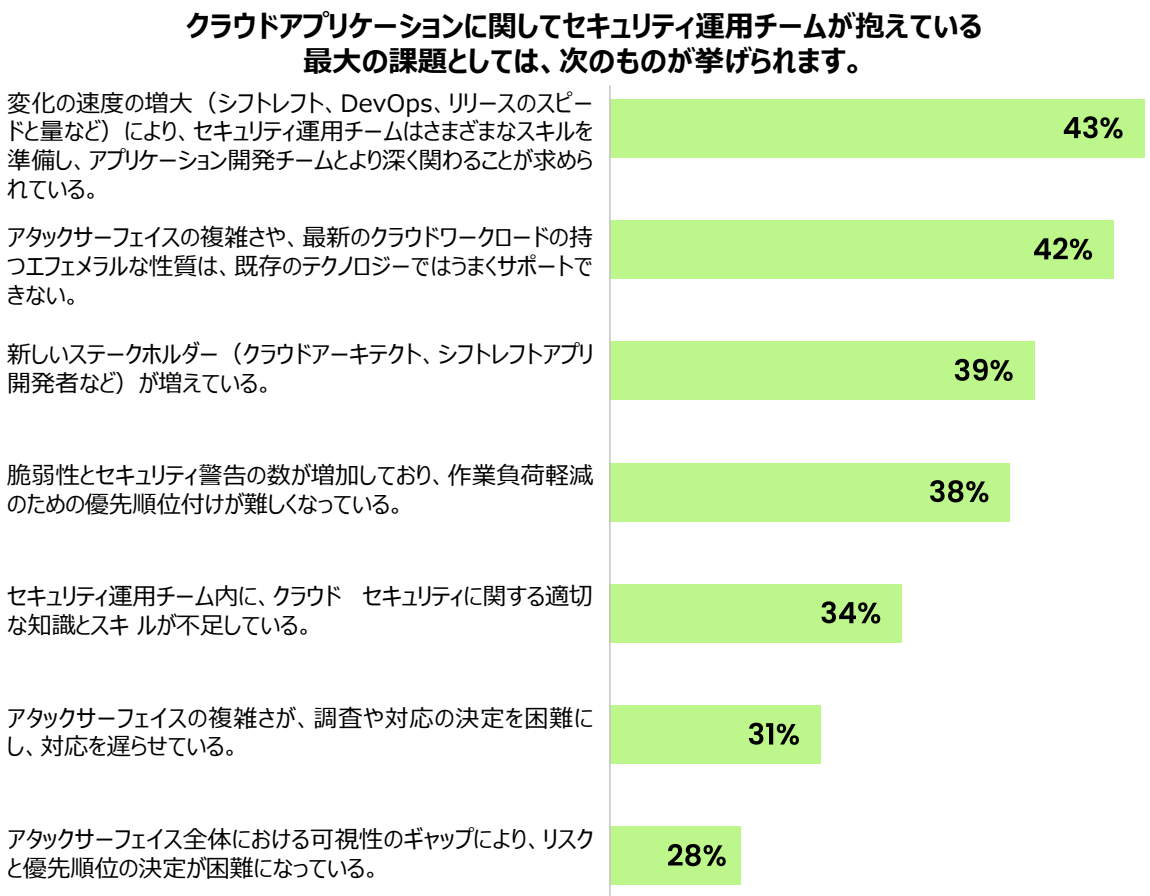


図1：クラウドアプリケーションに関してセキュリティ運用チームが抱えている最大の課題'

出典：
ESG Cloud Detection and Response: Market Growth as an Enterprise Requirement
Melinda Marks, Senior Analyst Jon Oltsik, Distinguished Analyst and ESG Fellow July 2023.

2024年、データ侵害の平均総コストは、2023年の445万ドルから488万ドルへと増加しました。見逃されているセキュリティインシデントは、単なる業務上のダウンタイムにとどまらず、多大な損害をもたらします。また、深刻な情報漏洩は、事業の損失、顧客の喪失、罰金、そして事後処理や被害対策に費やされる多額の費用につながる可能性があります。

クラウドの侵害がビジネスに及ぼす潜在的な影響を考慮すると、防御を強化し、必要なツールを配備するための措置を講じることが極めて重要となります。

インシデント対応に対する従来のアプローチでは、アナリストが詳細情報を検索することや、より深い調査のために問題の処理を上位レベルへと引き渡す為にで、遅延が発生します。生成AI（GenAI）は、生産性の向上とビジネス問題の解決を目指す企業や組織にとっての最優先事項として浮上してきました。生成AIは、クラウドセキュリティチームがクラウドセキュリティ上の問題を理解しそれに対応できるようにチームを支援することに関して、大きな可能性を秘めています。

クラウドでの検知と対応における555ベンチマーク（検知に5秒、相互関連付けに5分、対応に5分を推奨する基準）」は、最新の攻撃の現実を企業や組織に認識させるものです。Sysdigでは、555ベンチマークを満たすことにより、侵害の可能性を低減し、エスカレートした脅威の深刻度を抑えることで、侵害リスクを41%低減できると試算しています。

クラウドセキュリティの専門家として訓練されたAIセキュリティアシスタントは、あらゆるスキルレベルのスタッフが脅威を理解し、迅速かつ効率的に対応し、555ベンチマークを達成できるように支援することに関して、大きな可能性を秘めています。しかも、これらはすべて、AIアシスタントとのシンプルな会話を通じて実現されます。

41%
555ベンチマークを
満たすことによる
侵害リスクの削減率

クラウドでの検知と対応における555ベンチマーク ➡

AIがセキュリティに与える影響を測定する

セキュリティリーダーは、スキルギャップを解消し、インシデント調査を迅速化し、コストを削減するために、AIと自動化ソリューションに注目しています。IBMは、最新の年次**データ侵害コストレポート**の中で、AIを活用した企業や組織は、平均220万ドルのコスト削減を実現していることを明らかにしています。

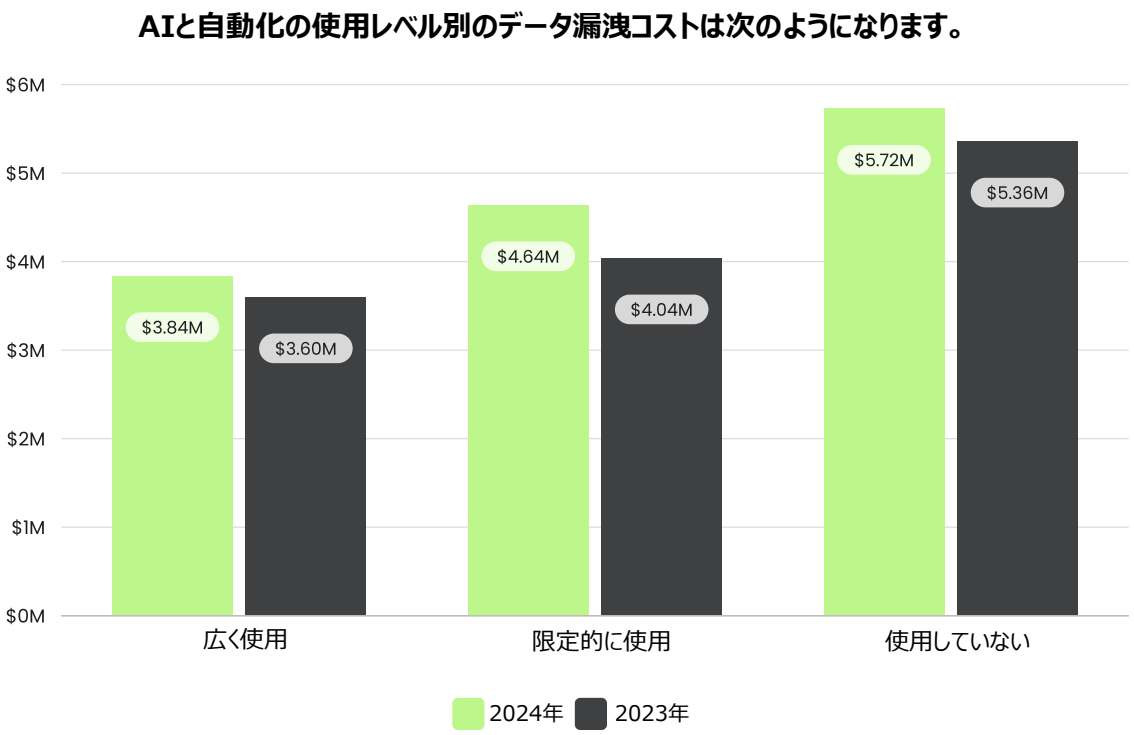


図2：AIと自動化の利用レベル別のデータ漏洩コスト

出典：IBM Cost of a Data Breach Report 2024

また、IBMは、AIと自動化の活用により、調査と対応に要する平均特定時間（MTTI）と平均封じ込め時間（MTTC）が30%短縮されたと報告しています。

AIクラウドセキュリティアナリストである Sysdig Sageが持つビジネス価値

Sysdigが開発したAIクラウドセキュリティアナリストである**Sysdig Sage**は、単純なAI要約にとどまらず、クラウドセキュリティインシデントの分析においてセキュリティチームを支援します。Sysdig Sageは、Sysdigクラウドセキュリティプラットフォームの統合コンポーネントとして、長時間に及ぶ調査を迅速かつ有意義な会話に変えます。これにより、セキュリティチームはイベントの原因の追究と、検知された脅威を阻止するためのソリューションに集中できるようになります。

Sysdig Sageは、多段階推論とコンテキスト認識の利用により、会話を通じてユーザーとの対話をサポートします。Sysdig Sageを使うと、あらゆるスキルレベルのスタッフが、業界に関する知識やSysdig脅威リサーチチームの持つ専門知識を活用できるようになります。Sysdig Sageは、ユーザーに、高度なクラウド脅威が持つ複数の層を 1 つずつ明らかにしていき、セキュリティインシデントを封じ込めるための次の防衛策を実現するための推奨事項を、コンテキストに沿って即座に提供します。

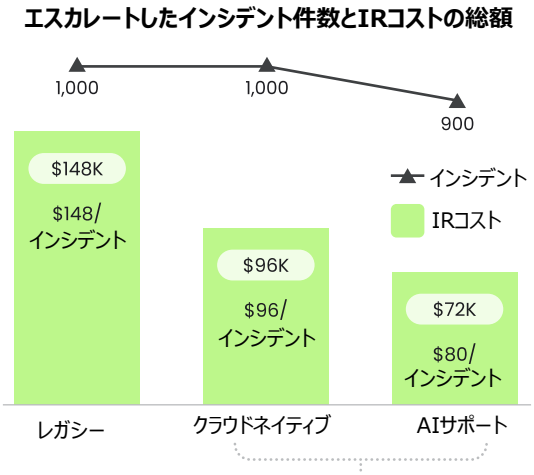
Sysdigは、米国の大手銀行とSysdigプラットフォームとSysdig Sageがインシデント対応コストに与える影響を定量化しました。

- Sysdigは、インシデント対応にかかるコストを、従来のプロセスに比べて52%削減できると見積もっています。
- コスト削減の16%は、AIによる生産性向上がもたらしたものです。
- インシデント1000件あたりの推定運用コストは、Sysdig Sage導入前には14万8000ドルでしたが、導入後は7万2000ドルに減少しました。
- インシデントのエスカレーションが最大19%削減され、セキュリティオペレーションセンター（SOC）スタッフの総労働時間が388時間短縮されました。

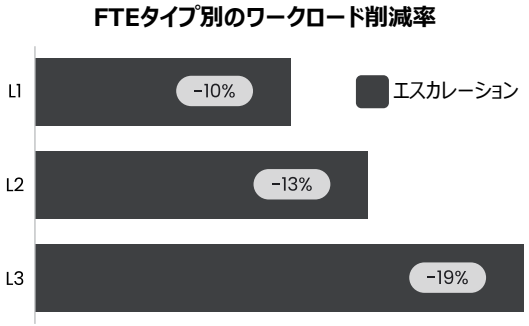
このように、Sysdig Sageで調査を行うと、セキュリティアナリストの貴重な時間を節約できると同時に、経験の浅いアナリストもより多くの作業を行えるようになります。この結果、インシデント管理コストを大幅に削減することが可能となります。

現在、データ侵害の世界での平均コストは488万ドルであり、攻撃が未解決のまま放置されると、被害額は1日あたり数万ドル増加することになります。Sysdig Sageは、セキュリティチームによる調査と対応作業を支援することで、インシデントが侵害に拡大するのを防ぎ、関連する経済的な影響を最小限に抑えるか、または排除することを可能にします。

米国トップ5の銀行における1,000件のセキュリティインシデント（レガシー）の概要



SysdigのCNAPPとAIにより、インシデントあたりのコストを**52%**削減



L1～L3 SOCアナリスト間でのエスカレーションの**減少**

＊FTE（L1～L3、年俸12万5,000～17万5,000ドル）あたり、0.5～4時間のレガシーIR期間を短縮

図3：米国のトップ5銀行における1,000件のセキュリティインシデントの概要

出典：銀行とSysdigによる分析

クラウドセキュリティのための生成AIにより、セキュリティ専門家の対応力を強化

クラウドエコシステムとテクノロジースタックは非常に複雑になっており、クラウドセキュリティチームは脅威への迅速な対応という大きなプレッシャーにさらされています。パブリッククラウドとプライベートクラウド、コンテナ、そしてKubernetesの複雑な仕組みをナビゲートすることは、熟練した専門家にとってもコストがかかり、困難な作業となります。AIアナリストは、これら専門家の集合知と、AIモデルによる継続的な学習を即座に提供できます。これにより、コスト削減とリスク削減がもたらすメリットを目に見える形で享受できるようになります。

Sysdig Sageは、専用に構築されたAIクラウドセキュリティアナリストであり、人による対応を加速します。対応に要する時間が数分しかない場合、サイバーセキュリティイベントを理解し、それに対応するのに役立つ会話が行えることは非常に強力な機能です。Sysdig Sageは、誰もが簡単にサイバーセキュリティを利用できるようにすることで、大きなビジネス価値を提供します。Sysdig Sageは、Sysdigプラットフォームのリアルタイム性を最大限に活用することで、次のことを実現します。

- 調査の合理化
- インシデントのエスカレーションを減らす
- あらゆるレベルの従業員がより多くのことを行えるようにする

> “Sysdig Sageは、人的ミスを劇的に減らし、何百時間も節約してくれます。当社では、Sysdig Sageを導入することで、ランタイムセキュリティ問題の掘り下げや、防止策を検討するための時間を劇的に短縮できました。
>
> 米国大手銀行エンジニアリング部門バイスプレジデント

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける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。Sysdigは、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、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項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。

sysdig

BUSINESS VALUE BRIEF

PB-040-JA REV. A 10/24