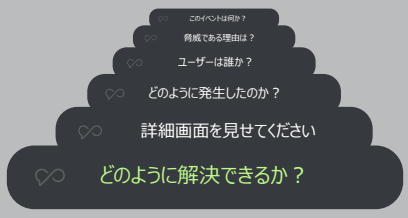
Sysdig Sage™：初の会話型AIクラウドセキュリティアナリスト

人によるクラウド脅威への対応を高速化



クラウド攻撃はより素早く、より巧妙に進化しています。そして、AIや自動化を攻撃者が利用する場合、リスクはさらに高まるばかりです。予防だけでは十分ではありません。進行中の攻撃を阻止するには、防御者がリアルタイムで攻撃の全体像を調査して把握できるようにする必要があります。

セキュリティチームには、無駄な時間はありません。情報を探している間の対応の遅れは、攻撃者により多くの時間を与え、データとワークロードをより大きなリスクにさらすことになります。

Sysdig Sageは、自律型のエージェントアーキテクチャーを搭載しており、マルチステップ推論とコンテキスト認識型でインシデントを徹底的に分析します。これにより、Sysdig Sageは、複雑なクラウド攻撃の解決を高速化します。

“

これは、AIが私たちのためにずっとやってきたはずのことです。それは、人の持つ対応能力を高め、かつ高速化することです。

最高情報セキュリティ責任者

BIGCOMMERCE

会話を通じて対応を高速化

対応に数分しか余裕がない場合でも、Sysdig Sageによりセキュリティチームは、迅速かつ有意義な会話へと変えることで、長時間の調査を短縮して最も重要な作業に集中できるようになります。

AIの専門家チームによる防御の強化

Sysdig Sageは、自律型のエージェントアプローチを採用しています。Sysdig Sageが利用している専門分野に特化したAIエージェントは、まるで専門家チームのように連携して動作します。これを利用することで、クラウドセキュリティに関する幅広い課題に対応できるようになります。

あらゆるスキルレベルでクラウドセキュリティを管理

Sysdig Sageを使うと、スキルレベルに関係なくSysdigの提供するリアルタイムのクラウドセキュリティプラットフォームを活用できるようになります。Sysdig脅威リサーチチームが提供する最新の知見を活用し、誰もが最大限に活用できるようになります。

AIを活用したクラウドの検知と対応を通じて、より迅速に攻撃を阻止し、よりスマートに業務を遂行

Sysdig Sage for CDRを使うと、パブリッククラウドおよびプライベートクラウド環境全体におけるランタイムのセキュリティイベントに関するインサイトを迅速に入手できるようになります。これにより、すべてのユーザーにとってサイバーセキュリティをより容易なものにすることが可能となります。

このイベントは何か？
ユーザーは誰か？
どのように発生したのか？

マルチステップ推論

- 綿密なコミュニケーションを取りながら、高度なクラウド脅威の層を一つひとつ解明していくのを支援します。
- 簡単な質問から始めて、その後より深く掘り下げるためにフォローアップの質問をします。
- セキュリティイベントとその対応方法をより明確に理解します。

詳細画面を見せてください

コンテキスト認識型

- ユーザーが画面上で見ているものに基づいて、セキュリティに関する正確なインサイトを得ることができます。
- 簡単な質問をすることで、イベントの詳細を即座に知ることができます。
- AIが推奨するビューを使用して、ユーザーインターフェイスをナビゲートします。

本日発生した深刻度の高いイベントの要約

インサイトの生成

- コンテナ、Kubernetes、およびクラウド全体で検知されたイベントを要約して説明します。
- イベントに優先順位をつけ、分析を合理化し、早急な対応が必要な問題にプロアクティブに対処できるようにします。
- ランタイムイベントに関する詳細な情報を通じて、スキルギャップを埋めます。

どのように解決できるか？

ガイド付きレスポンス

- セキュリティイベントの管理方法に関するガイダンスと明確化を通じて、対応時間を短縮できます。
- セキュリティ対応、予防戦略、およびプロセス改善に関する積極的な提案を受け取ることができます。
- プラットフォームを離れることなく、クラウドセキュリティ脅威への対応を高速化できます。

sysdig SECURE EVERY SECOND.

PB-039-JA Rev. A 9/24

www.sysdig.com