sysdig Google Cloud

# Google Cloudのための クラウドセキュリティ

アプリケーションとインフラストラクチャーのモダナイズを目的としたGoogle Cloudにおける クラウドコンピューティングへの移行は、セキュリティに対する新たな要件をもたらします。 セキュリティチームは、目まぐるしく変化するクラウドの脅威を一歩先で防ぐための施策 を強化する必要があります。このガイドでは、Google Cloud環境を保護するためのベスト プラクティスを紹介するほか、SysdigとGoogleの提供するソリューションが、設定ミス、サプ ライチェーンの抱えるリスク、進化するサイバー脅威などの主要な課題への対処にいかに役 立つかを紹介します。

# 目次

03
はじめに
クラウドの保護における主な課題

04
Google Cloudのセキュリティアプローチ
脆弱性管理

07
クラウドセキュリティポスチャー管理

12
クラウドの検知と対応

15
クラウドセキュリティと生成AI

18
結論

# はじめに

クラウドでは、1秒1秒が重要です。Google Cloudを使用している企業や組織は、より速くイノベーションを起こすことできますが、その一方で、セキュリティに関しても後れを取らないようにする必要があります。

攻撃者が自動化やAIを活用するに従い、クラウドベースの攻撃速度が速くなっています。わずか**10分**で、被害がもたらされることもあります。クラウドセキュリティチームは、セキュアな状態を維持するために、かつてないほどに迅速かつ効率的に脅威を検知、調査、修正する新しい方法を見つける必要があります。

セキュリティ対策はクラウド特有の課題に対応するために絶えず進化しています。ポイントソリューションも、脆弱性管理やポスチャー管理からワークロードの保護に至るまで、さまざまな機能に対応するように進化しています。同時に、企業や組織は現在、クラウドセキュリティ手法を統合するようなプラットフォームを採用することに価値を見出しています。このようなアプローチを通じて、クラウド、コンテナ、およびホスト全体におけるリスクを可視化するための単一ビューを実現できるようになります。

クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）は、シグナルを相互に関連付ける一連のセキュリティ機能を統合します。これにより、開発から運用に至るまで、クラウドとコンプライアンスの全体像をより完全にかつ効率的に把握できるようになります。また、脆弱性管理、ポスチャー管理、権限およびエンタイトルメント管理、脅威検知、インシデント対応を一元化することで、効率化を促進し、クラウドのリスクに先手を打つことが可能となります。

このガイドでは、Google Cloudへの投資リスクを低減し、セキュリティを確保するためのソリューションをナビゲートするためのフレームワークを提供します。また、Google Cloudが提供するソリューションについて説明するほか、Google CloudのセキュリティをSysdigの提供するCNAPPソリューションがどう補完するかを紹介します。

# クラウドの保護における主な課題

クラウドを利用することで、セキュリティチームはボタンをクリックするだけでインフラを構成し、ワークロードを展開できるようになります。このような変化のスピードはリスクへの扉を開くものであり、特に脅威アクターはクラウドの自動化のスピードを悪用することで、数分で攻撃を開始できるようになっています。また、新たな予期せぬ可視性のギャップが、セキュリティとコンプライアンスを複雑にする可能性があります。

- **設定ミスとヒューマンエラー：**設定ミスはクラウドにおける重大な懸念事項です。クラウドのリソース、権限、サービスが誤って設定されると、機密データの漏洩や、不正アクセスが発生する可能性があります。
- **ソフトウェアサプライチェーンが抱えるリスク：**攻撃者は、開発、デプロイ、導入の各プロセスにおいてソフトウェアを標的にします。多くの場合、悪意あるコードの導入や脆弱性の悪用を防ぐための効果的なセキュリティ対策を実施できていません。
- **進化するサイバー脅威：**サイバー犯罪者は、クラウド環境への標的手法を常に進化させています。Webアプリケーション、API、ユーザーインターフェイスなどのような多数のエントリーポイントを持つ複雑なインフラストラクチャーは、不適切な設定や監視が行われないまま放置されるとリスクをさらす可能性があります。

# Google Cloudのセキュリティアプローチ

クラウドセキュリティを成功させるには、ソフトウェア開発ライフサイクル全体を幅広くカバーする能力と、既知および未知の脅威から身を守るための深い分析能力が必要となります。すなわち、ホストやコンテナからサーバーレス環境に至るまでをカバーする能力と、クラウドサービスやアイデンティティの領域でリアルタイムに起きていることと情報を相互に関連付ける能力が鍵となります。

クラウドセキュリティプログラムでは、しばしば「シフトレフト」および「シールドライト」という2つのアプローチが強調されます。

- **シフトレフト**型のアプローチは、セキュアな設計を促進するプロセスとツールに焦点を当てるものであり、プレリリーステストを通じて、本番環境で問題となる前にセキュリティ上の問題を特定します。このアプローチは、DevOpsのプラクティスと関連付けられます。
- **シールドライト**型のアプローチは、運用プラクティス、セキュリティ監視、セキュリティインシデントを防止する仕組み、そして発生したイベントを検知して対応する仕組みに重点を置くものです。

シフトレフトとシールドライトという2つのセキュリティ上のプラクティスは、Google Cloudのセキュリティを確保するために不可欠です。

- **クラウドワークロード保護（CWP）：**コンテナ、Kubernetes、ホストを保護するほか、脆弱性を特定して優先順位を付け、サーバーレス型のワークロードを保護します。
- **クラウドセキュリティポスチャー管理（CSPM）：** 設定ミスにフラグを立て、それらの修正を自動化します。セキュリティとコンプライアンスに関する進捗状況を継続的に追跡します。
- **クラウド検知と応答（CDR）：コ**ンテナ、Kubernetes、およびクラウド全体における攻撃パターンを検知します。ランタイムの脅威からワークロードを保護します。

上記のソリューションに組み込まれている重要なプラクティスは、すべてGoogle Cloud用のクラウドネイティブアプリケーション保護プラットフォーム（CNAPP）に集約されています。以降のセクションでは、CNAPPの主な機能を紹介します。これらの機能はすべて、お客様がお使いのGoogle Cloud環境でエンドツーエンドのセキュリティを実現するのに役立ちます。

---

# 脆弱性管理

脆弱性管理は、クラウド上で実行されるワークロードのセキュリティにとって極めて重要な側面です。ソフトウェアの欠陥と既知のセキュリティ問題のスキャンは、CSPMとCWPPの両プラクティスにとって鍵と見なされている機能であり、セキュリティ侵害を防止するために、アプリケーションライフサイクルに必須のステップです。

新たな脆弱性が常に公開され続けています。包括的な脆弱性評価のアプローチを採用することは、ソフトウェア開発ライフサイクル（SDLC）全体を通じて問題を特定し、それに対処するための鍵となります。

最新のアプリケーションのセキュリティを評価するには、問題を早期に発見して修正することが必要となります。これは、開発段階でスキャンを行い、実行時に至るまで脆弱性のスキャンを継続することを意味します。各段階で問題をチェックすることにより、以前の段階で見落とされた脆弱性、実行時に導入された脆弱性、および最後のスキャンの後に開示されたリスクを特定できるようになります。

フルライフサイクルの脆弱性管理とは、さまざまな段階や場所で問題をスキャンすることを意味します。これには次のスキャンが含まれます。

- 開発者マシン上でのローカルスキャン
- CI/CDパイプラインのスキャン
- レジストリのスキャン
- ランタイムのスキャン

## シフトレフトにおけるセキュリティ上の課題

シフトレフト型のセキュリティにはノイズの問題があります。企業や組織は、プレリリーススキャンツールを使って作業を開始しますが、すぐにスキャナー出力の洪水に溺れてしまいます。アプリケーションリリースの合否を判断する効率的な方法を見つけるのは一苦労です。

開発チームとセキュリティチームは、調査結果を入念に吟味することで、重大で対処可能な欠陥に優先順位を付ける必要があります。この作業は面倒であり、より重要なタスクから時間を奪うことになります。セキュリティテストの落とし穴に対処するのは簡単ではありません。これらのチームは、個々の調査結果に関連するリスクについて推論を始めるには、できるだけ多くのコンテキストに関する情報を必要とします。

### Google Cloudの脆弱性管理ソリューション

Google Cloudは、ソフトウェアの脆弱性を特定するソリューションを提供しています。同ソリューションを使うと、クラウドチームは、脆弱性を発見した後、脆弱性に関する調査結果を適切なチームにルーティングすることで、セキュリティとコンプライアンスを向上できます。

**Artifact Analysis：**ソフトウェアトウェア構成分析およびスキャンサービスであり、Artifact RegistryやGoogle Kubernetes Engine（GKE）など、多くのGoogle Cloud製品における既知の脆弱性を特定します。

**Mandiant Attack Surface Man-agement：**外部アタックサーフェスにおける脆弱性や設定ミスを特定した上で、最新のサイバー攻撃への対策を常に把握できるようにします。

## SysdigによるGoogle Cloudの脆弱性管理

Sysdigは、開発プロセスにおけるさまざまな段階やランタイムに**脆弱性管理**を組み込んでいます。また、Sysdigを使う事で、Google Cloudユーザーはリスクに優先順位を付けることが可能となるほか、ホストとコンテナのイメージスキャンを単一のワークフローへと統合することで、時間とコストを節約できるようになります。

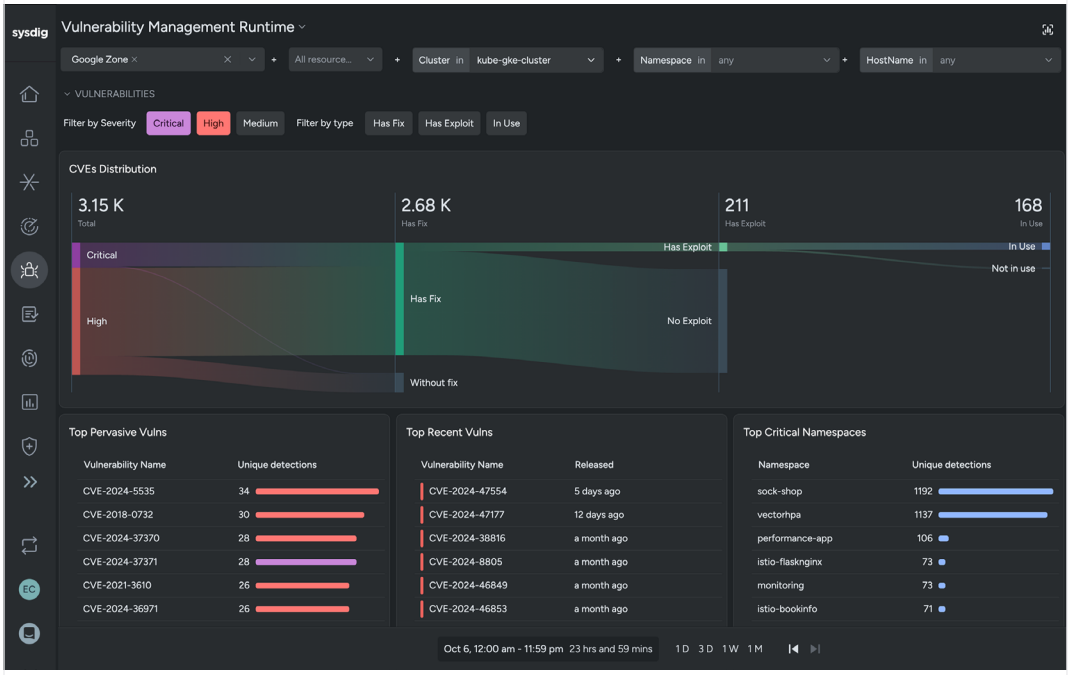
- **CI/CDパイプラインのスキャン：**CI/CDパイプラインにおける脆弱性スキャンは、レジストリにプッシュする前のビルドステップとして、コンテナイメージを評価します。追加のゲートとして、セキュリティポリシーの評価に合格しないビルドを失格させることができます。
- **レジストリスキャン：**レジストリスキャンは、Google Cloud上での本番運用の前に、コンテナイメージと成果物に脆弱性が含まれていないかどうかを確実にチェックします。
- **ランタイムスキャン：**実行時に脆弱性をスキャンすることで、それ以前の段階で特定されなかった問題、実行時に導入された問題、または前回のスキャン実施後に公開された問題を特定します。

#### ランタイムインサイトを使用した脆弱性の優先順位付け

脆弱性を突く脅威を一歩手前で防ぐためには、使用中の脆弱性パッケージと休止中の脆弱性パッケージを識別するためのコンテキストを追加する必要があります。これにより、ノイズを減らし、実際のリスクに注目することが可能となります。Sysdigの**ランタイムインサイト**は、コンテナをプロファイリングし、この情報を脆弱性管理とアプリケーションセキュリティ（AppSec）ツールで利用できるようにすることで、このような可視性を実現しています。

ランタイムインサイトにはSysdigのCNAPP内でアクセスできますが、サードパーティのAppSecソリューションでもランタイムインサイトを利用できます。**Snyk**、**Checkmarx**、**Docker**のようなAppSec業界のリーダー企業は、Sysdigとの統合を通じて、使用中の脆弱性に優先順位を付け、脅威をより迅速に排除する機能を提供しています。

図1：
ランタイムの脆弱性管理




**エージェントレス型のスキャンとエージェントベースのスキャン**

企業や組織はしばしば、必要な機能を提供するためにエージェントをインストールして保守することを躊躇しがちです。可能であれば、チームはエージェントレス型のアプローチを利用することを望みます。エージェントレス型のセキュリティスキャンは、通常、クラウドプロバイダーのAPIを利用して情報を収集し、脆弱性評価を行っています。

エージェントレス型スキャンの欠点として、通常リアルタイムの可視性を提供しないことが挙げられます。つまり、前回と今回のスキャンの間におけるシステムの中間状態に関する情報が提供できない可能性があるのです。さらに、エージェントレス型のスキャンは、通常、脆弱なパッケージがランタイム環境で使用されているかどうかについてのインサイトを提供できません。

Sysdigは、エージェントレス型スキャンとエージェントベースのスキャンという2つのオプションを統合しています。

- エージェントレス型のスキャンは、Google Cloud APIを利用してリソースを見つけてスキャンします。
- エージェントベースのスキャンは、軽量パッケージを使用して、ノードベースのスキャンとランタイムの可視性の両方を提供します。

両方のオプションを併用することも可能です。このアプローチでは、エージェントはワークロードをプロファイリングし、使用中のパッケージを特定します。この情報は、エージェントレス型のスキャナーにより、脆弱性の優先順位付けをする際に使用されます。

詳しくは、**クラウドの保護：効果的な脆弱性管理へのガイド**をご覧ください。

# クラウドセキュリティポスチャー管理

Gartner® によると、「2025年までに、クラウド侵害の99%以上は、顧客の設定ミスやミスが根本原因となるだろう」[1] とのことです。クラウドセキュリティポスチャー管理（CSPM）を利用すると、自社のクラウド設定に関する可視性を確保することで、リスクの特定と修正を行い、Google Cloud環境をプロアクティブに保護できるようになります。

## セキュアなクラウド構成を保証

クラウドセキュリティ戦略の要となるのが、ポスチャー管理です。クラウドの設定ミスは、ビジネスをリスクにさらします。ホスト、コンテナランタイム、クラスター、ストレージ、またはクラウドリソースの設定を誤ると、権限昇格やラテラルムーブメントの実行が容易になります。Google Cloudのアカウントとサービスをベンチマークとポスチャー管理に照らして評価することで、リソースがセキュリティのベストプラクティスから逸脱している場合には検知することができます。

CSPMソリューションでは、クラウド構成の評価と修復を手作業で行うのではなく、クラウド構成の状態を自動的に評価した上で、リスクのある設定ミスを出力できます。場合によっては、CSPMは、欠陥のある設定を更新するかまたは無効化することで、修復を自動化できることもあります。

## IaC（Infrastructure-as-Code）の保護

Terraformのようなツールを使ったIaC（Infrastructure-as-Code）は、クラウドにおけるITプロビジョニングおよびIT管理の中心的な要素となっています。IaC設定を検証することは、CSPMにおけるもう1つの重要な構成要素です。

IaCセキュリティツールとプラクティスを利用することで、エンジニアは、IaCテンプレート内でセキュリティ上の問題を発見して修正できるようになります。その目的は、IaCを通じて不注意にセキュリティ問題を引き起こすリスクを最小化することです。IaCセキュリティは、セキュリティリスクを軽減するために設計されたガバナンスを導入するという意味で、ポスチャー管理の一部となります。

## Kubernetesのセキュリティポスチャー管理

Kubernetesセキュリティポスチャー管理（KSPM）とは、セキュリティ自動化ツールを使用することで、Kubernetesのあらゆるコンポーネント内のセキュリティとコンプライアンスの問題を発見して修正するものです。KSPMは、Kubernetes環境におけるCSPMであると見なすことができます。KSPMは、Kubernetesの監査ログに加えて、Kubernetesのリソースおよびホスト構成を分析します。KSPMを利用することで、クラウドネイティブなインフラストラクチャーにおけるセキュリティリスクの防止と修正が行えるようになります。

Google Kubernetes Engine（GKE）のようなクラウドマネージド型のKubernetesサービスでは、Google CloudがKubernetesの制御プレーンを管理します。このため、セキュリティポスチャーはGoogle Cloudによって管理されます。ワーカーノードなど、GKE環境にけるその他の側面については、ハードニング、パッチの適用、セキュリティアップデートの管理について責任を負います。完全なセルフホステッド型のKubernetes環境の場合、環境全体のセキュリティポスチャーを管理する必要があります。

1 Gartner, Risk-Based Evaluations of Cloud Provider Security, Charlie Winckless, Jay Heiser, 16 January 2023.
GARTNERは、米国およびその他の国におけるGartner, Inc.および/またはその関連会社の登録商標およびサービスマークであり、この文書では許可を得て使用しています。無断複写転載を禁じます。

## パーミッションとエンタイトルメントの管理

過剰な権限を付与されたクラウドアカウントやクラウドロールは、もう1つの重大なセキュリティ問題を引き起こします。IAM（アイデンティティおよびアクセス管理）は、Google Cloudユーザーがアクセスをロックダウンして、データ漏洩、権限昇格、ラテラルムーブメントのリスクを回避するために不可欠な機能です。

Google Cloudのサービスや機能の利用が増えるにつれ、最低限必要な権限を正確に把握することがより困難になります。つまり、権限が誤って設定されることや、不要なアクセス権が許可されることが多くなるのです。

適切な権限を慎重に割り当てることは、クラウドにおけるアイデンティティリスクに対処し、Google Cloud環境における最小権限の実践を達成するための基礎となります。CIEM （Cloud Infrastructure Entitlement Management）は、重要なCSPM機能の1つと見なされており、クラウド環境における権限の維持に伴う複雑さに対処するために特別に設計されています。

**98%**

**Sysdigの2024年版クラウドネイティブセキュリティおよび利用状況レポート**によると、付与された権限の98%が未使用であることが判明しています。

### Google Cloudの提供するCSPM、IaC、CIEMソリューション

ポスチャー管理とコードセキュリティのためのGoogle Cloudソリューションを使うと、クラウドチームは、セキュリティに関する調査結果を集約し、構成とコードを分析し、権限の問題を特定できるようになります。

**Security Command Center：**プロアクティブなセキュリティとリアクティブな（事後対応型の）セキュリティを統合し、コード、アイデンティティ、データに対するポスチャー管理と脅威検知を提供します。

**Security Health Analytics：**Security Command Centerが提供するマネージドサービスの1つであり、クラウド環境をスキャンし、攻撃にさらされる可能性のある一般的な設定ミスを検知します。

**IAM Recommender、Security Health Analytics、および CIEM：**これらのサービスは、アイデンティティとアクセスに関する調査結果を生成します。これらは、Security Command Centerが持つCIEM 機能の一部と見なされます。

**Policy Analyzer：**IAM許可ポリシーに基づいて、ユーザー、サービスアカウント、グループ、ドメインに付与されているGoogle Cloudアクセス権を可視化します。

# Sysdigが提供するGoogle Cloudのポスチャー管理

SysdigのCSPMソリューションは、クラウドの制御プレーン、クラウドリソース、クラウド上に展開されたワークロード、および権限における設定ミスを特定して修復を可能にすることで、クラウドインフラストラクチャーとアイデンティティに関するリスクを継続的に管理します。

**セキュリティに関するベストプラクティスとコンプライアンス**

Sysdigを使うと、セキュリティおよびコンプライアンス標準、一般的なフレームワーク、規制要件、および社内ポリシーに照らして、対象となる環境をプロアクティブに評価できます。

Sysdigは、下記の標準を含む80件以上のビルトイン型のポスチャー評価機能をサポートしています。

| | | | | |
|---|---|---|---|---|
| CIS Google Cloud Platform Foundation ベンチマーク | CIS Google Kubernetes Engine (GKE) ベンチマーク | Center for Internet Security (CIS) Benchmarks for Linux、Kubernetes、Dockerなどのベンチマーク | Defense Information Systems Administration (DISA) Security Technical Implementation Guide (STIG) | Digital Operational Resilience Act (DORA) |
| Federal Risk and Authorization Management Program (FedRAMP) | 一般データ保護規則（GDPR） | Health Insurance Portability and Accountability Act (HIPAA) | H ealth Information Trust Common Security Framework (HITRUST CSF) | ISO/IEC 27001 |
| National Institute of Standards and Technology (NIST) | Network and Information Security (NIS) Directive (NIS2) | NSA/CISA Kubernetes Hardening Guide | Payment Card Industry Data Security Standard (PCI DSS) | System and Organization Controls (SOC) 2 |


図 2：Google Cloudのセキュリティポスチャーレポート

Sysdigプラットフォームは、お使いのクラウドにおける完全なインベントリを検出して提示します。これにより、IaaS、PaaS、ホスト、コンテナ、脆弱性、アイデンティティなどを含む資産のリスクとコンプライアンスを評価できるようになります。また、静的なリスク要因（公開情報やアクセス許可など）と動的なリスク要因（使用中のパッケージなど）の両方に基づいて、資産の検索とフィルタリングが行えます。

**アクティブなクラウドリスク**

クラウドの導入が加速するにつれ、CSPMの要件も変化しています。業界は、クラウドのアクティブなリスクを特定し、優先順位を付け、軽減するために、定期的なポスチャーチェックから継続的なポスチャー評価へと移行しつつあります。静的なチェックは重要ですが、クラウドにおける攻撃のスピードを考えると、このような定期的なポイントインタイム型の評価では、数時間以上に及ぶ可視性のギャップが生じる可能性があります。

アクティブな動きや動的な変化を見つけるために、Sysdigはアクティブなクラウドリスクを発見して軽減する機能を提供します。アクティブなクラウドリスクには、お使いの環境における、次のようなリアルタイムの活動や動的な変化が含まれます。

- 危険なIDの振る舞い（例：MFAなしでユーザーがアクティブにログイン）
- リアルタイムの設定変更（例：既知の悪意あるネットワークへの接続）
- 使用中の権限（例：事前に使用されていない高権限アクセスの有効化）
- 重大な脆弱性を持つ使用中のパッケージ（例：重大なCVSSの脆弱性を持つソフトウェアパッケージがアクティブに実行されている）
- ワークロードの脅威（例：公開暗号鍵のアップロード）

Sysdigは、静的リスクの調査結果をリッチ化した上で、アクティブなリスク情報を重ね合わせることで、優先順位付け、調査、修復を実現します。Google Cloudに対する静的なリスクとアクティブなリスクの最も危険な組み合わせは、攻撃経路の可視化を通じて上位に表示されるため、調査が迅速化されます。また、ワークフローに統合されたガイド付きの修正機能を利用することで、セキュリティチームは問題を迅速に修正できるようになります。

Attack Path Analysis（攻撃経路分析）の可視化により、静的なリスクにアクティブなリスクやイベントを重ね合わせながら、リソース間の相互接続リスクや悪用可能なリンクを表示できます。

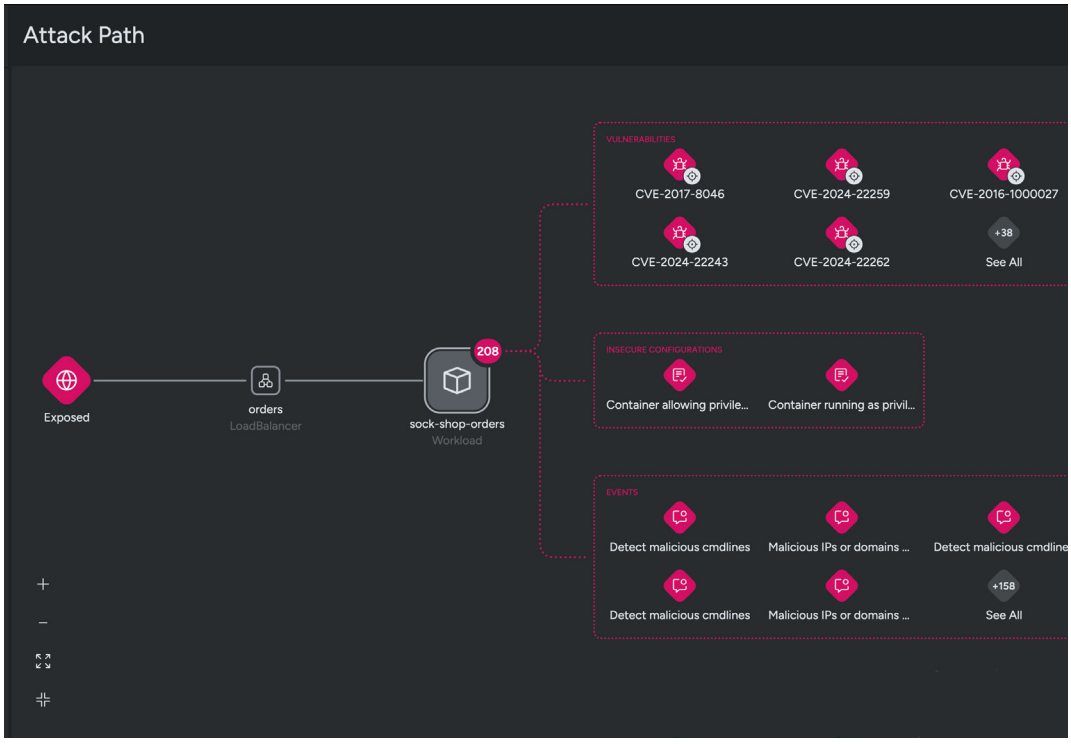



図3：
リアルタイム
インサイトによる
クラウド攻撃
経路の可視化

**IaC（Infrastructure-as-code）のセキュリティ**

Sysdig は、資産とリソースを、IaCマニフェストファイルへとマッピングします。これにより、セキュリティに関するインサイトを提供し、ドリフト検知を可能にし、環境内における違反を修正することが可能となります。発見された違反に対して、Sysdigはカスタマイズされた修正案を生成します。この修正案を利用することでGitツールとの統合を通じて、プルリクエスト経由で問題を修正できます。

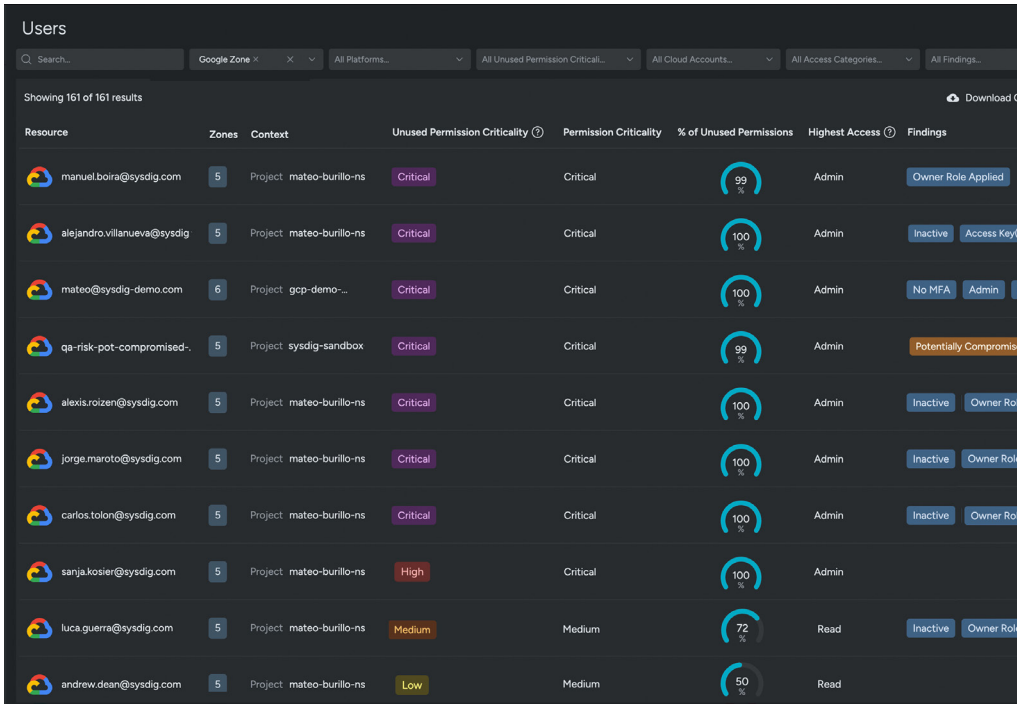
**エンタイトルメント管理**

Sysdigは、お使いのクラウド権限を分析することで、クラウドユーザー、ロール、ポリシーに関するプロファイルを作成します。監査ログの分析により、Google Cloudアカウントで実行されたクラウドコマンドを明らかにし、このアクティビティとポリシー、ロール、ユーザーを相互に関連付けます。このような可視性により、権限の悪用リスクをもたらす可能性のある、過剰な権限を付与されたアイデンティティを把握できるようになります。

アイデンティティおよびアクセスダッシュボードは、次の情報を提供します。

- 付与された権限と使用された権限の合計
- 何名のユーザーが非アクティブであり、どのユーザーの削除を検討すべきか
- ポリシーごとの権限数とユーザーごとのポリシー数の平均値
- 最悪のケースをもたらす可能性のある未使用の権限を持つポリシー、ユーザー、ロール

図4：
Google Cloudの
エンタイトルメント
および権限管理




Sysdigは、パーミッション分析をポリシーの提案へと変換します。この提案を利用することで、過剰に付与された権限を削減し、付与されたアクセス権を、必要とされるものに対するアクセスのみに制限できます。

Google Cloudにおける効果的なポスチャー管理の詳細については、**最新のCSPMソリューションに不可欠な5つの機能**をご覧ください。

# クラウドの検知と対応

クラウド攻撃の阻止は、企業や組織がより大規模で複雑なクラウド環境に移行し続ける中で、セキュリティチームに必要とされる重要な能力です。クラウド攻撃の検知と対応は、しばしば、レガシーなEDRツールに起因するノイズや可視性のギャップによって中断されることがあります。クラウドサービス、エフェメラルなコンテナ、アイデンティティの無秩序な増加は、ダイナミックで複雑な環境をもたらしています。そのような環境を保護することが困難であるのは明らかです。

脅威は、わずか数分で脆弱性を悪用します。クラウドの検知と対応（CDR）は、クラウドインフラとデータを標的とするサイバー攻撃に対するプロアクティブな防御を提供します。これには、潜在的な脅威に対するクラウドシステムの継続的な監視、深刻度の評価、調査能力、影響を防止または軽減するための対策の実施などが含まれます。

効果的なCDRの鍵となるのは、ワークロード、アイデンティティ、クラウドサービス、サードパーティアプリにまたがる悪意あるアクティビティをリアルタイムで特定し、クラウドファブリック全体における脅威を検知する能力です。

マイクロサービスアーキテクチャーとは、コンテナ上で動作し、Kubernetesのようなソリューションによってオーケストレーションが行われる仕組みであり、これを利用すると、アプリケーションの開発を高速化し、スケーリングが容易になります。しかし、その一方で、コンテナアクティビティの監視は飛躍的に複雑になります。コンテナは複数のインスタンスやホストに分散され、分離されたコンテキストでプログラムを実行します。アクティビティを可視化するには、独自のインスツルメンテーションが必要です。セキュリティインスツルメンテーションは、リアルタイムでデータを収集できる必要がありますが、可視性を得るためにコンテナイメージを変更する必要はありません。

企業や組織は、テクノロジーを採用するだけでなく、プロセスを確立した上で、クラウドシステムとデータをセキュアに保つために、迅速に行動するのに必要となるスキルをスタッフに身に付けさせる必要があります。

適切なCDR戦略を導入することで、Google Cloudユーザーは次のことが可能になります。

- 侵害リスクの低減
- コンプライアンス要件を満たす
- 検知と対応に要する時間を短縮
- コストの削減、生産性の向上、イノベーションをセキュアに加速

クラウドチームが検知と対応のセキュリティ戦略の指針として活用できる主要なセキュリティフレームワークの1つとして、MITRE ATT&CKフレームワークが挙げられます。このフレームワークは、攻撃者の振る舞いや手法に関する詳細で実用的な情報を提供するものであり、進化し続ける環境の中でセキュリティチームがクラウド資産をプロアクティブに保護するのに役立ちます。

詳しくは**MITRE ATT&CK and D3FEND for Cloud and Containers**をお読みください。

## わずか10分で攻撃が発生

標的型クラウド攻撃は、クレデンシャルの検出から平均で10分以内に発生します。

## Google Cloudの脅威検知、調査、対応ソリューション

Google Cloudの提供する脅威検知、調査、対応ソリューションを使うと、クラウドの脅威を検知し、ワークロード、アプリケーション、データに関するセキュリティをより完全に把握できるようになります。

**Event Threat Detection（イベント脅威検知）：**
Security Command Center Premium層に組み込まれているサービスであり、プロジェクトを監視し、システム内の脅威をほぼリアルタイムで特定します。

**Google Security Operations（旧称Chronicle）：**
この機能を使うと、セキュリティチームは、セキュリティ関連のテレメトリを内密に保持し、分析し、検索できるようになります。これにより、リスクのある活動を特定した上で、脅威から身を守ることが可能となります。

## SysdigによるGoogle Cloudのクラウド検知と対応

SysdigのGoogle Cloud向けの検知および対応（CDR）機能は、アナリストが加速する複雑なクラウドの脅威から組織を守れるようにすることに重点を置いています。この機能により、セキュリティチームは、クラウドとクラウドネイティブなワークロード向けに構築されたディープな可視性、コンテキスト、リアルタイムの検知機能を確保できます。

**オープンソースソフトウェアのFalco**をベースに構築されたSysdigのCDRは、クラウドログ、コンテナ、Kubernetes、サーバーレスコンピューティング、およびクラウドホスト全体における高度な検知と対応機能を提供します。SysdigのCDRはリアルタイムで脅威を検知し、複数のドメインにまたがるコンテキストを相互に関連付けます。これにより、アナリストは、脅威の迅速な調査、特定、対応が行えるようになります。

### Google Cloudサービスのセキュリティ

Google Cloudは、200件を超えるクラウド サービスを提供しています。これには、コンピュート、ストレージ、データベース、アナリティクス、ネットワーク、開発者ツール、管理ツール、セキュリティ、エンタープライズアプリケーションなどが含まれており、幅広いユースケースに対応しています。**Google Cloud Audit Logs**は、Google Cloudアカウントの運用監査とリスク監査を実現するために、ユーザー、ロール、クラウドサービスによって実行されたアクションを記録します。これは、Google Cloudサービスにおけるセキュリティを実現するための重要なコンポーネントの1つです。

クラウドサービスやクラウドインフラストラクチャーの利用が拡大する中、Sysdigを利用すると、柔軟なセキュリティルールセットを使用して、クラウド監査ログイベントの評価をリアルタイムに自動化できるようになります。また、CloudTrailのログを継続的に監視することで、さまざまなGoogle Cloudサービスにおける不審なクラウドのアクティビティやイベントを検知して報告できるようになります。

### Google Cloudコンテナサービスのセキュリティ

Sysdigは、コンテナセキュリティに関する広範な専門知識を有しており、Google Cloud上のコンテナ（**Google Kubernetes Engine**や**Cloud Run**など）に関する深いな可視性を提供します。これにより、脅威の検知、攻撃の阻止、インシデントレスポンスの迅速化がより容易になります。

Sysdigは、カーネルレベルのインスツルメンテーションを採用しており、最も包括的なランタイムセキュリティをコンテナに提供します。これには、プロセスの生成、ファイルシステムのアクティビティ、ネットワークトラフィックなどに関する可視性が含まれています。カーネルレベルのインスツルメンテーションは、ユーザースペースのプログラムと比較してオーバーヘッドが少ないため、システム全体への影響を軽減できます。

Sysdigエージェントは、コンテナランタイムAPIとKubernetes APIにネイティブに統合され、メタデータの収集と生成されたイベントのリッチ化を可能にします。検知されたイベントには、コンテナ名、所属するKubernetesクラスター、ポッド、ネームスペース、サービス/デプロイメントなど、影響を受ける資産に関する広範な情報が含まれます。クラウドアカウント、クラウドリソースタイプ、セキュリティグループ、リージョンなどを相互に関連付けるためにGoogle Cloudアカウントを接続すれば、さらなるリッチ化が可能となります。

ポリシーにより、特定のアクティビティが検知された場合、コンテナを停止して脅威を即座にブロックできます。さらに、イベント前、イベント中、イベント後のすべてのシステムアクティビティを記録するキャプチャファイルを保存することにより、イベント後のフォレンジックと調査を実現できます。

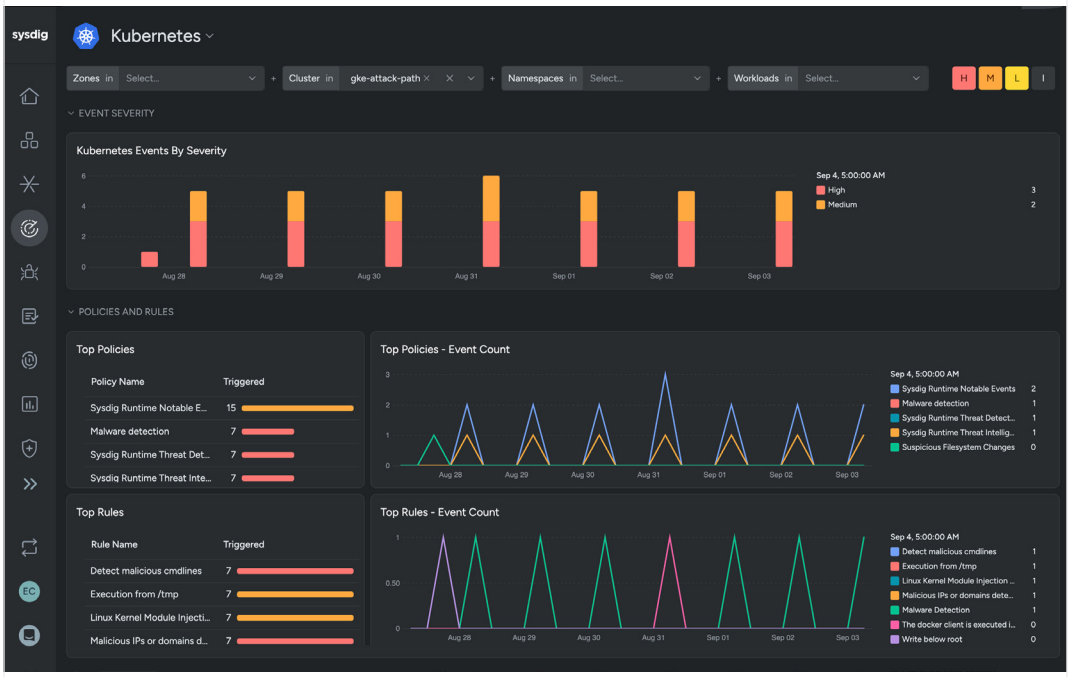



図5:
Kubernetesと
コンテナセキュリティの概要

**Google Cloud Runにおけるサーバーレス型コンテナのセキュリティ**

サーバーレスコンピューティングでは、検知と対応に独自の要件が伴います。サーバーのホストオペレーティングシステムにアクセスできない場合、従来のエージェントベース型のインスツルメンテーションは利用できません。Sysdigは、**Google Cloud Run**におけるサーバーレス可視性の課題を独自の方法で解決します。

- サーバーレス型のワークロードエージェントは、各Cloud Runタスクのセキュリティイベントを監視し、セキュリティおよびコンプライアンス ポリシーを適用します。
- サーバーレス型のオーケストレーターエージェントは、サーバーレス型のワークロードエージェントから情報を収集し、SysdigのSaaSバックエンドクラウドへと送信します。これにより、セキュリティチームはイベントを表示した上で、それに対処できるようになります。

セキュリティイベントをSIEMやセキュリティデータレイクへと転送

セキュリティ情報およびイベント管理（SIEM）およびデータレイクソリューションを使うことで、セキュリティ運用チームは、組織内のさまざまなソースから大量のセキュリティ関連データを保存できるようになります。これらのデータは、セキュリティの監視、分析、コンプライアンスなどのユースケースに使用されます。

Sysdig はGoogle Security Opera-tions（SecOps）（旧称 Chronicle）を含む多数のSIEMおよびデータレイクソリューションとの統合が可能であるため、Sysdigを使うと、強化されたマルチプラットフォームのクラウドセキュリティイベントをGoogle Cloudに保存した上で、選択した分析ツールを使用してセキュリティデータを分析できます。

## クラウドの検知と対応における 5/5/5ベンチマーク

クラウドにおける実際の攻撃のスピードを考慮すると、ユーザーは新たな方法でその有効性を測定する必要があります。Sysdigが提唱する「5/5/5ベンチマーク（検知 5秒、トリアージに5分、対応 5分）」は、Google Cloudユーザーに最新の攻撃の現実を認識し、クラウドセキュリティプログラムを推進することを要求するものです。5/5/5ベンチマークを達成するには、攻撃者が攻撃を完了するよりも速く、クラウド攻撃を検知して対応する能力が必要となります。

- **5秒以内に脅威を検知：**エフェメラルな資産に関する可視性を確保するために、クラウドセキュリティツールからリアルタイムで検知シグナルを収集できる必要があります。
- **5分以内に相互関連付けとトリアージを実施：**最初の関連アラートを受信してから5分以内に、相互に関連連付けられているすべてのシグナルにおける完全なコンテキストを収集できる必要があります。
- **5分以内に対応を開始：**攻撃が進行中であることを確認してから5分以内に戦術的な対応を開始できる必要があります。

詳細については、「**555ベンチマークを達成するには**」をご覧ください。

---

# クラウドセキュリティと生成AI

生産性の向上とビジネス上の問題の解決を目指す企業にとって、生成AI（GenAI）は最優先事項です。AIは、リスクとセキュリティの問題に対するチームの理解を深めることで、クラウドセキュリティを支援し、セキュリティ運用と対応時間を短縮する可能性を秘めています。同時に、企業はGenAIやLLM（Large Language Model）アプリケーションの運用に伴う独自のサイバーセキュリティリスクを管理する方法を見つけなければなりません。

## AIが抱えるセキュリティリスク

生成AIは大きな可能性を秘めていますが、プライバシー、サイバー攻撃、規制コンプライアンス、知的財産の侵害など、数多くのセキュリティリスクも伴います。AIの出現によって、脅威アクターが高度な攻撃を実行し、AIシステムを操作してシステムの整合性を侵害するための障壁が低くなる可能性があると考える人もいます。

AIにより膨大な量のデータが使用されかつ生成されるようになるため、不正アクセスや悪用、さらにはプライバシー規制に違反する可能性などの問題から身を守る必要があります。これらのリスクに対処するには、AIのセキュリティ、機密性、整合性を維持することで、不正アクセスや有害事象を防止、検知、対応するための最善の方法を慎重に決定する必要があります。

## 生成AIとLLMにおけるコンプライアンスフレームワーク

AIが世界中のビジネスや社会のさまざまな側面にとって不可欠なものになるにつれ、プライバシー、消費者の権利、国家安全保障などの分野への影響に対する懸念が高まっています。AIの持つ広範な影響を管理し、関連するリスクを軽減するために、AIの安全、プライバシー、倫理的な使用を保証するためのガバナンスフレームワークとベストプラクティスが開発されています。

**NIST**、**Mitre**、**OWASP**などの組織が開発しているフレームワークは、AIを導入する企業が既知のリスクや誤用から身を守るための支援を目指すものです。さらに、世界中でAIセキュリティ規制が策定中であるか、またはすでに実施されています。これらの取り組みは、AIがもたらす機会と課題の両方に対処するという、より広範な世界的なトレンドをサポートしています。

詳細については、「**AIのガバナンスをめぐる競争**」をご覧ください。

## セキュリティアシスタントとしてのAI

Google Cloudユーザーは、セキュリティ運用を強化してリスクの優先順位付け、対応の迅速化、クラウドセキュリティの簡素化を図るために、生成AI（GenAI）と大規模言語モデル（LLM）に注目しています。AIは実用的なインサイトを生成し、このインサイトを利用してリスクとセキュリティの問題をより深く理解することで、セキュリティの運用と対応にかかる時間を短縮できます。さらに、生成AIは、経験の浅いセキュリティ担当者でも複雑なタスクを処理できるようになり、プロアクティブなリスク調査を通じて全体的なサイバー防御を強化できる可能性を秘めています。

### セキュリティ関連のGoogle Cloud AIソリューション

Google Cloudは、AIの使用を保護するソリューションと推奨事項を提供しているほか、生成AIを使用してクラウドセキュリティを支援するためのソリューションと推奨事項を提供しています。

**GoogleのSecure AI Framework（SAIF）：**モデルのリスク管理、セキュリティ、プライバシーなどのAIの懸念に対処し、AIの利用が「セキュアバイデフォルト」であることを保証するように設計されています。

**脅威検知における Gemini：**Google のSecLM API上に構築されたAIを活用した機能を提供するものであり、Mandiantの最前線の脅威インテリジェンスを活用して、脅威アクターの行動に関するインサイトと概要を提供します。

**Google SecOpsにおける Gemini：**自然言語を使用してクエリを生成し、セキュリティデータと会話することで調査を実施し、イベントの修正を支援します。

## Sysdigのセキュリティソリューションと AI

### SysdigによるAIワークロードのセキュリティ

Sysdigは、生成AIを安全に導入するのに役立つAI Workload Securityを提供します。これにより、セキュリティチームは自社の環境内にあるAIワークロードを識別して優先順位を付けることができます。これには、Googleの**Vertex AI**や**Gemini**などの主要なAIエンジンやサポートソフトウェアパッケージのサポートが含まれます。

AI Workload Securityは、データセキュリティ対策を確立するために必要となる可視性を提供します。これにより、AIワークロードへの不正アクセスを通じて企業秘密、専有情報、顧客データが漏洩するリスクに対抗できるようになります。相互に関連付けられたリスクとイベントを包括的に把握することで、次のようなリスク要因を迅速に把握できるようになります。

- 公開されているAIワークロード
- 重大な脆弱性のある使用中のAIパッケージ
- 信頼性の高い脅威イベント

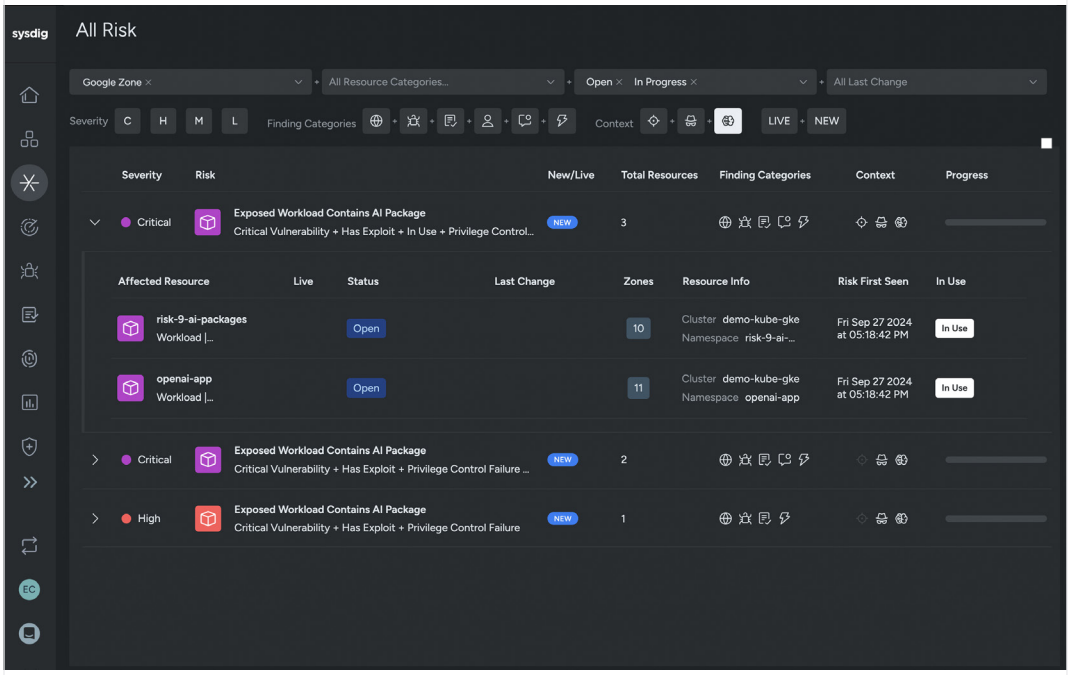



図 5：
Google Cloudの
AIワークロードセキュリティ

詳細については、**Sysdig's AI Workload Security**をご覧ください。

## Sysdig Sage™：最初のAIクラウドセキュリティアナリスト

パブリッククラウド、プライベートクラウド、コンテナ、Kubernetesの保護の複雑さに対処するのは、複雑な仕事です。経験豊富な専門家であっても、最新のクラウドの脅威に先手を打つことは困難です。

Sysdig Sageは、SysdigのAIクラウドセキュリティアナリストです。Sysdig Sageは、人間のような会話を通じてユーザーと対話し、セキュリティイベントの実像を明らかにするのに役立ちます。Sysdig Sageは、人間の専門家の集合知とAIモデルの継続的な学習を即座に提供し、Google Cloudユーザーがセキュリティの問題に迅速に対応できるようにします。

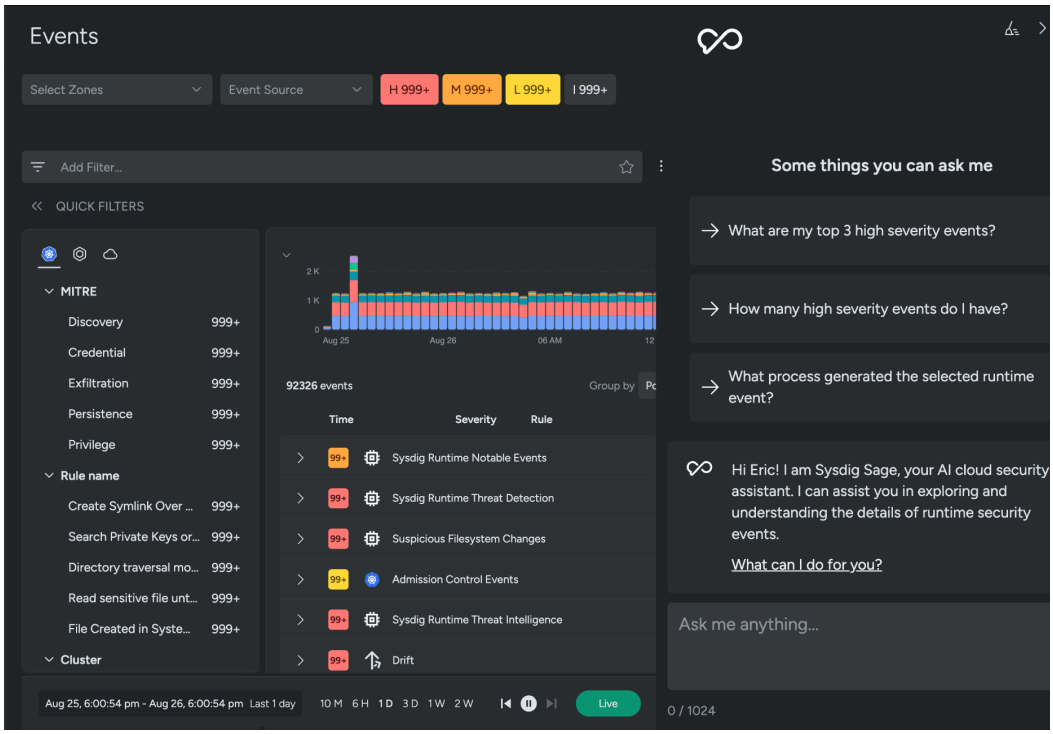



図6:
Sysdig Sage-AI
クラウド
セキュリティアナリスト

Sysdig Sageの詳細については、**こちら**をご覧ください。

## 結論

Google Cloudは、企業や組織が迅速に行動し、イノベーションを起こして、顧客と市場のニーズを満たすようなソリューションを提供できるよう支援しています。企業や組織がクラウドの利用を拡大するにつれて、セキュリティプラクティスも進化しているため、増え続ける脅威に対応するための対策を取り込む必要があります。堅牢なクラウドセキュリティにより、リアルタイムの可視性を実現できるほか、インサイトを相互に関連付けて対応を迅速化する機能を統合できます。SysdigプラットフォームのようなCNAPPソリューションを利用すると、Google Cloudユーザーは、セキュリティをモダナイズし、脅威が拡大する前に先手を打って鎮静化することで、クラウド環境をセキュアに維持できます。

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。

Sysdig. Secure Every Second.

詳細はこちら ➡

sysdig

GUIDE

COPYRIGHT © 2025 SYSDIG,INC.
ALL RIGHTS RESERVED.
GUIDE-013-JA REV. A 1/25