sysdig

# オープンソースで構築されたクラウド脅威検知

## 最新のクラウド環境におけるランタイムセキュリティ

Falcoは、コンテナ、Kubernetes、クラウドサービス全体の脅威と異常をリアルタイムで検知するためのオープンソースソリューションです。セキュリティカメラとして機能し、予期せぬ動作、設定変更、侵入、データ窃取をリアルタイムで継続的に検知します。FalcoはSysdigが開発し、Cloud Native Computing Foundation（CNCF）に寄贈されました。実践されたテクノロジーであり、確立された組織に属するユーザーや利用者同士で形成された力強いコミュニティで急成長し、そのダウンロード数は、1億件を超えています。

堅牢なオープンソース基盤上でユーザーは、Falcoのルール言語がもたらす新しい検知における透明性と俊敏性を享受できます。

SysdigのCNAPP（クラウドネイティブアプリケーションプロテクションプラットフォーム）は、Falcoをベースに構築されています。オープンソースのFalcoはクラウドネイティブの脅威を検知するために使用されるものですが、Sysdig Secureはさらにクラウドインフラの保護に役立つ機能を追加して提供しています。Sysdigは、Falcoの機能をすべて強化することで、運用を簡素化しているほか、ユーザーが大規模環境においてFalcoから最大限の力を引き出せるようにしています。

> 「Falcoは事実上、セキュリティソリューションのスタンダードです。Falcoを利用することで私たちは、クラウドおよびコンテナ向けのランタイムセキュリティにおける業界標準を導入したのだということを認識しました。Falcoのオープンソースコミュニティとドキュメントを利用できたことは、当社にとって非常に有益でした。」
>
> セキュリティアーキテクト BEEKEEPER

## メリット

### エンタープライズグレードのサポート

Sysdigの専門家が提供するテクニカルサポートを通じて、Falcoから最大限の力を引き出せるようになります

### 操作性

ルール管理、イベント管理、統合、自動化されたルールの調整

### 高度な脅威検知

Sysdigの脅威リサーチチーム（Sysdig TRT）が厳選したカスタムルール/ポリシーと脅威フィードに基づく検知

### 調査と対応

すべての対話型コマンドとシステムコールをキャプチャすることで調査を加速し、リモートシェルを経由して環境内で直接トラブルシューティングを実施

### パフォーマンスの向上

大規模環境向けに最適化されたメタデータ収集により、エージェントのフットプリントを削減

# Falcoから最大限の力を引き出す

Sysdigの製品は、Falcoを中核に検知とランタイムインサイトを実現しており、これは一連のセキュリティソリューションの原動力となっています。Sysdigは、簡素化された運用と大規模環境への拡張性を持ってユーザーがFalcoを最大限に活用できるよう支援しています。また、Sysdig Secureは、CSPMや脆弱性管理などの追加機能を通じて、予防から防御に至るまで、クラウドネイティブ環境におけるエンドツーエンドのカバレッジを提供します。

| | sysdig | Falco |
|---|---|---|
| オープンソースベースのエージェント | ✓ | ✓ |
| **脅威検知** | | |
| イベントソース（システムコール、K8s監査ログ、クラウドログ） | ✓ | ✓ |
| アラート出力 | ✓ イベント転送 | ✓ Sidekick経由 |
| カスタマイズ可能なポリシー | ✓ | ✓ |
| 自動化されたルール調整 | ✓ | |
| 自動化されたポリシー提案 | ✓ | |
| K8sネットワークセキュリティ | ✓ | |
| **その他の機能** | | |
| 脆弱性管理 | ✓ | |
| IACセキュリティ | ✓ | |
| CSPM（攻撃経路分析、インベントリ、リスクの優先順位付け） | ✓ | |
| コンプライアンス（「すぐに使える」タイプ） | ✓ | |
| 監査/フォレンジック | ✓ | |
| エンタープライズグレードのサポートとスケーラビリティ | ✓ | |
| Snykとの統合 | ✓ | |

sysdig


PB-035-JA REV. A 4/24

Secure Every Second.

**Sysdigの動作を見る**

デモを依頼 →