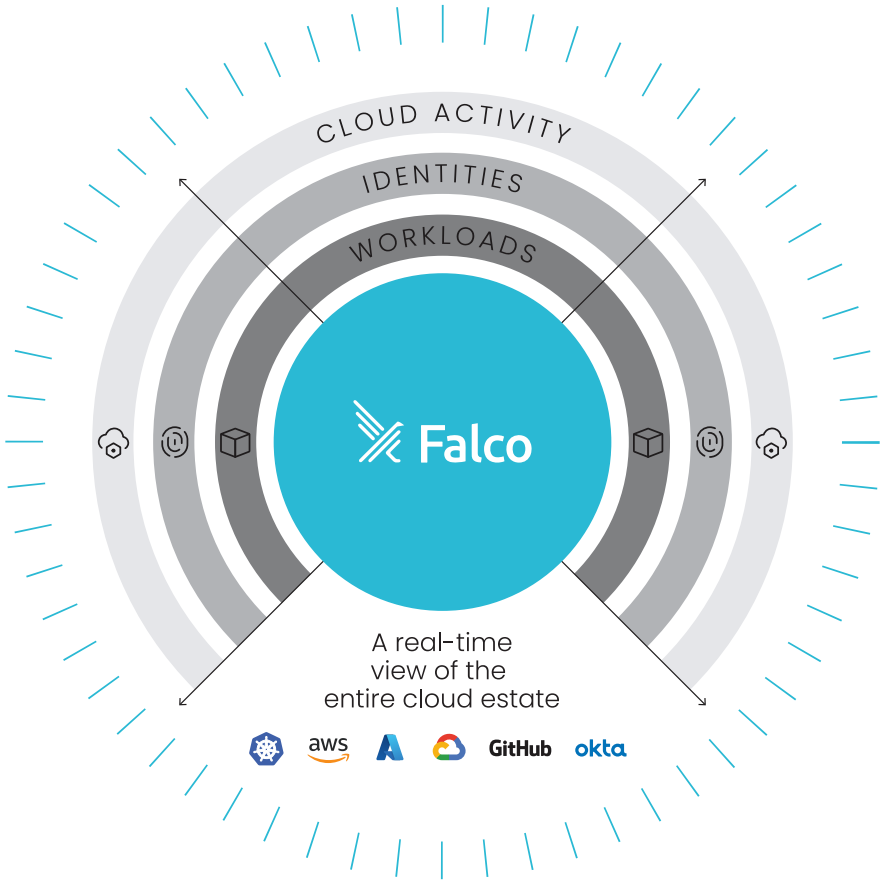
EBOOK

クラウドの保護：
エンタープライズエクスペリエンスにおける
Falcoのメリット

sysdig SECURE EVERY SECOND.

2016年に初めてリリースされて以来、Falcoはコンテナ、クラウド、およびKubernetesにとって最適な脅威検知エンジンとなっています。1億3,000万以上ダウンロードされたFalcoは、主要なクラウドプラットフォームを通じて、大手のテック企業、クラウドプロバイダー、そしてスタートアップ企業に採用されています。



SysdigはFalcoの生みの親であり、Falcoのメンテナーとして、このオープンソースの脅威検知エンジンを強力かつ誰にとっても利用しやすいツールにすることに尽力しています。Falcoは、最初のランタイムセキュリティプロジェクトとして2018年にCNCF Sandboxに受け入れられました。正式にGraduate（卒業）となるため（すなわちCNCFで最高の地位を獲得するため）に、Falcoプロジェクトは、約6年にわたる厳しいデューデリジェンスプロセス、つまりCNCF技術監視委員会（TOC）チームによって監視されました。このプロジェクトは、Falcoの成長と成熟度を検証するために、第三者によるセキュリティ監査を完了したのです。これにより、同プロジェクトの地位は、クラウドネイティブな脅威検知における事実上のスタンダードとして確固たるものとなりました。

Sysdigは、Falcoをベースとして独自のクラウド検知および対応エンジンを構築しました。Falcoの先進的な脅威検知エンジンとSysdigの包括的な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）を組み合わせることで、脅威を検知できるだけでなく、脅威を調査し、クラウドスピードで脅威に対応できるようになります。

ここからは、FalcoにおけるSysdigのマネージド型脅威インテリジェンスを活用することで、クラウドとコンテナのセキュリティをリアルタイムで向上させている海外企業の事例をご覧ください。

Case Study

ICG Consulting社、クラウドにおける開発をセキュアに加速

AWSとFalcoの両方を利用していた当社は、強力なマルチレベルのセキュリティ戦略を有しており、コンプライアンスに準拠したネットワーク全体でセキュリティを確保していました。しかし、規模を拡大するにつれ、Sysdigを採用することは当社にとって自然な成り行きでした。Falcoをベースとしたテクノロジーの持つ強みと、SysdigのAWSとのパートナーシップを考慮すると、Sysdigを採用することにより、さらに迅速にサービスを提供できることが分かっていました。

— ICG Consulting社、テクニカルコンサルタント

導入前の課題

ICG Consultings社は、バックオフィスアプリケーションのエキスパートとして長年の信頼を得ている企業です。ICGが顧客に提供するクラウドベースのサービスがセキュアであることを保証するために、同社はFalcoを使用していました。しかし、ICGのクラウドサービスが成長するにつれ、開発を遅らせることなく、クラウドセキュリティを簡素化する方法が必要となりました。

導入効果

クラウドセキュリティを拡大し、Falcoと並行してSysdigプラットフォームを採用することで、ICGはクラウド、コンテナ、ホスト全体における可視性を高め、ノード、ポッド、ユーザーレベルで問題を迅速に特定できるようになりました。わずか数週間のうちに、ICGはセキュリティを犠牲にすることなく、アラートの量を30%削減できました。

15% クラウドリソースにおけるコスト削減

10% リリースのペースが毎週増加

Case Study

BlaBlaCar社、開発者にセキュリティリスクの管理を支援

FalcoのユーザーがSysdigによるFalcoへの貢献から恩恵を受けているように、Sysdigの顧客もコミュニティによる貢献から恩恵を受けています。SysdigがFalcoを拡張するという事実は、当社にとって実に魅力的でした。当社は、Sysdigを利用することで、Falcoと統合された最高のツールを入手できると確信していました。

— BlaBlaCar社、セキュリティエンジニア

導入前の課題

BlaBlaCar社は、世界トップクラスのコミュニティをベースとしたトラベルネットワークを運営しています。Google Cloud Platform（GCP）とGoogle Kubernetes Engine（GKE）に120以上のノードを追加することを決定した後、同社は、開発者が本番環境でアプリケーションの構築と実行を行えるようにする、新しいセキュリティソリューションを必要としていました。

導入効果

Sysdigの導入により、BlaBlaCar社の開発者は不審なアクティビティや設定ミスを迅速に特定することでリスクを低減できるようになり、その結果、セキュリティチームがより効率的に仕事を行えるようになりました。さらに、SysdigはFalcoの強力な機能に加えて、専門的なサポートとSaaSインフラを提供するため、セキュリティチームは、セットアップやメンテナンスに時間を費やすことなく、統合に集中できるようになりました。

200人以上 の開発者が、アプリケーションのライフサイクル全体にわたって管理し責任を持つように

効率的でセキュアなDevOpsモデルによりオーバーヘッドを削減

SysdigとFalcoを通じてクラウドスピードで脅威を管理

すべての企業や組織がFalcoからSysdigへの移行を望んでいるわけではなく、Falcoのままでも問題はありません。なぜなら、Falco Feeds by Sysdigの導入により、Falcoによるクラウドの保護が容易になっているからです。Falco Feeds by Sysdigを利用することで、本番環境におけるオープンソースのFalcoの導入に影響を与えることなく、進化し続けるクラウドネイティブ脅威の一歩先を行くことが可能となります。Falco Feedsは、脅威リサーチチームから継続的にアップデートされるルールを提供するほか、規制遵守のためのタグ付け、明確に定義された除外によるノイズの削減、さらには高度な検知コンテキストなどの機能を取り込んでいます。このため、Sysdigを導入することなく、完全にアップデートされた検知ルールセットを通じて、エンタープライズレベルの脅威検知に対するスムーズなアプローチを確保できます。

Falco Feeds by Sysdigを使うと、オープンソーススタックを維持しつつ、1秒1秒をいかに保護できるかをご覧ください。

詳細はこちら →

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。

Sysdig. Secure Every Second.

sysdig

E-BOOK

EBK-014-JA Rev. B 3/25