sysdig

ホワイトペーパー

エンドツーエンドの検知によりクラウドを保護

急速に進化する今日のテクノロジー環境では、クラウド環境、コンテナ、サプライチェーンがデジタルトランスフォーメーションを推進しており、強固な脅威検知を確保することは、かつてないほど困難になっています。また、コンテナ、ホスト、クラウドプラットフォーム、ID、サプライチェーンにまたがる多層インフラストラクチャーの台頭により、セキュリティに対する統一的なアプローチが必要となっています。このような複雑なセキュリティ状況の中、革新的なオープンソースプロジェクトであるFalcoと、同プロジェクトの創始者であるSysdigが、エンドツーエンドの検知機能を提供するパイオニアとして登場しました。Falcoは、Wiresharkに始まるイベントキャプチャとフォレンジックにおける20年の経験に基づき、最新のクラウドアーキテクチャーをしっかりと念頭に置いて構築されたものです。

企業や組織は、クラウドネイティブアーキテクチャーを採用し、多様な環境にアプリケーションを導入する中、多くのセキュリティ課題に直面しています。モノリシックなアーキテクチャー向けに設計された従来のセキュリティ対策では、最新のアプリケーションの動的で分散した性質を効果的に保護することは困難です。脅威はさまざまなレイヤーの脆弱性を突くことが可能となっているため、セキュリティと脅威の検知に対する統一的なアプローチを採用することが不可欠となっています。

Sysdig Secureの中核には、Falcoの統合検知エンジンが据えられています。この最先端のエンジンは、リアルタイムの振る舞い洞察と脅威インテリジェンスを活用することで、多層インフラを継続的に監視し、潜在的なセキュリティ侵害を特定します。コンテナの異常な動作、不正アクセスの試み、サプライチェーンの脆弱性、IDベースの脅威など、Sysdigを採用することで進化する脅威に対して統一的かつプロアクティブな防御策を確保できるようになります。

本稿では、攻撃によって脅かされるクラウドベースのアプリケーションとインフラの複数のレイヤーを見ていきます。また、Falcoを中核として構築されたSysdigのプラットフォームが、そのユニークな機能に基づいて、いかに優れたセキュリティを提供するかを紹介します。さらに、SCARLETEELエクスプロイトの調査を通じて、これらの機能が現実の侵害のコンテキストにおいて、いかに利用されるかを確認します。

目次

新たなクラウド脅威への挑戦

挑戦クラウド脅威の状況は、クラウド導入の増加、テクノロジーの変化、新たな攻撃ベクターの出現など、さまざまな要因によって、年々大きく進化しています。その進化の主な側面としては、次のものが挙げられます。

1. **アタックサーフェスの拡大：**システムやデータをクラウドに移行する企業や組織が増えるにつれて、アタックサーフェスが拡大しています。クラウド環境は、Webアプリケーション、API、ユーザーインターフェイスなど、多数のエントリポイントを持つ広大かつ複雑なインフラストラクチャーを提供します。攻撃者は、これらのエントリポイントの脆弱性を悪用することで、不正アクセスやサービス中断を行う機会をより多く手に入れています。
2. **攻撃の高度化：**サイバー犯罪者は、クラウド環境を標的とした、より高度な攻撃手法を開発しています。マルウェアやサービス拒否（DoS）攻撃といった従来の攻撃ベクターは依然として一般的ですが、攻撃者は、クロスアカウント攻撃やクロスクラウド攻撃をはじめ、コンテナやサーバーレス環境に固有の脆弱性を突いた攻撃、さらにはクラウドサービス事業者を標的としたサプライチェーン攻撃といった高度な戦術も採用しています。
3. **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あり続けています。クラウドのリソースやサービスが不適切に設定されることで、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。パスワードの脆弱性、アクセス制御の不備、クラウドストレージバケットの偶発的な露出などのヒューマンエラーは、データ漏洩や不正なデータ露出につながる可能性があります。
4. **コンプライアンスとガバナンスの課題：**データ保護法（GDPRなど）や業界特有のコンプライアンス基準などの規制要件に対応することにより、クラウドセキュリティ管理に複雑さが加わります。
5. **クラウドネイティブのセキュリティ課題：**コンテナやサーバーレスコンピューティングのようなクラウドネイティブテクノロジーには、独自のセキュリティ課題があります。コンテナの設定ミス、セキュアでないコンテナイメージ、サーバーレス機能の脆弱性などが攻撃者に悪用されることで、クラウド環境がハッキングされる可能性があります。このような動的かつエフェメラル（短命）なワークロードを保護するには、専門的な知識とセキュリティ対策が必要となります。
6. **不完全なツールでは目的を達成できない：**EDR（Endpoint Detection and Response）ツールは、ほとんどのセキュリティセンターにおける中核的なコンポーネントとなっています。EDRはワークステーションにおける従来の脅威に対しては効果的ですが、チームが同ツールをクラウドに適用しようとすると、可視性のギャップや不十分な保護機能が顕在化し始めます。EDRは、クラウド環境では効果がありません。なぜなら、クラウド環境は、多次元的でありかつ刹那的な複雑さ、膨大な量のデータ、そしてその変化の速さを特徴としているからです。

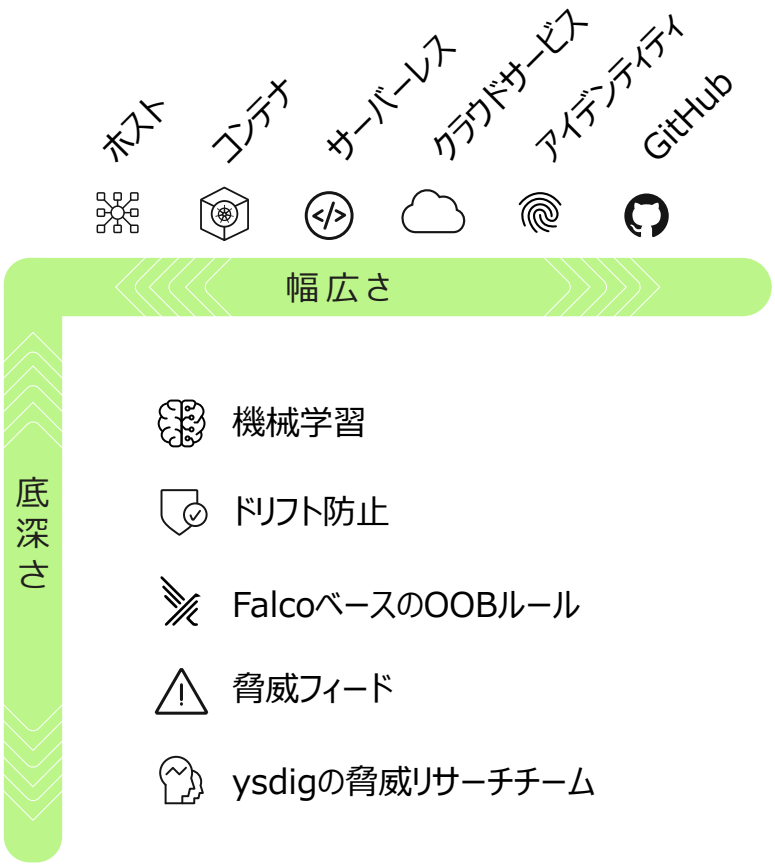
要約すると、クラウドの脅威の状況は年々大きく進化しており、組織はクラウドネイティブアプリケーション保護プラットフォーム（CNAPP）の一部として、多層的なアプローチによるクラウド検知・対応（CDR）を導入する必要があります。複数のセキュリティツールや技術を組み合わせることで、攻撃がもたらすリスクを低減し、クラウド上の機密データやアプリケーションを保護できるようになります。

クラウド攻撃対象領域の範囲

クラウド環境の保護は、ソフトウェア開発ライフサイクル全体をカバーする幅広さと、クラウドにおける既知および未知の脅威から保護するための分析の底深さを必要とするユニークな課題を提起しています。

カバレッジの観点からは、ホストやコンテナからサーバーレス環境まで対応していることが重要です。同じく重要となるのが、クラウドサービス、アイデンティティ、CI/CDプロバイダーで常に起こっていることとその情報とを相互に関連付けることです。一方、底深さという点では、従来のルールベースのエンジンを超えるようなアプローチをカバーする必要があります。Sysdigの専任の脅威リサーチチームは、最新の脅威に対応するルールを維持することに貢献しています。このようなプロアクティブなアプローチにより、進化する脅威状況に対応した最新の検知機能を維持できます。場合によっては、更新された脅威フィードを組み込むことで、新たに特定されたリスクに対するリアルタイムの保護を提供できます。

Sysdigが提供する底深くかつ幅広いカバレッジは、インフラのさまざまな部分から発生する脅威を統一されたアプローチで迅速に検知し、セキュリティプログラムが進化する脅威の状況に常に対応できることを保証します。本稿では、下記の図に示すすべての要素を取り上げています。



サーバー / クラウドホスト / VM

攻撃者は、クラウドホストの脆弱性や脆弱なセキュリティ制御を悪用して、不正アクセスや基盤インフラのハッキングを試みることがあります。ホストベースのランタイムセキュリティ、ログ分析、脆弱性ホストスキャンなどの多層的な検知メカニズムを利用することで、疑わしい活動を特定してブロックし、異常な動作を検知することにより、クラウド上のホストを標的とした攻撃に対するリアルタイムの保護を実現できます。

RedHatの調査によると、2020年に発生したKubernetesセキュリティインシデントの60%以上は、誤った設定や脆弱なホストに関連するものだったとのことです。これが、ホストレベルでディープなランタイム検知機能を持つことが不可欠である理由です。Falcoのエンジンは、お客様のサービスやアプリケーションが実行されている間にホストベースの脅威を検知するように設計されています。そうすることで、Falcoは異常で疑わしい振る舞いをリアルタイムで検知します。

Falcoの改良されたアーキテクチャー設計は、ストリーミングエンジンとして機能し、後のアクションのためにデータを保存するのではなく、到着時にデータを処理します。これにより、ホスト上でリアルタイムの検知機能を実現しています。また、Falcoはイベントシーケンスに基づいてアラートを生成するのではなく、各イベントを独立して評価することで、リアルタイム検知に関連して発生するオーバーヘッドを回避しています。さらに、Falcoはデータソースにできるだけ近い場所でルールを評価することで、データ転送の必要性を最小化し、アラートをできるだけ早くトリガできるようにすることを目指しています。

Falcoは、ホストベースの検知のためのデータのリッチ化にも重点を置いています。データのリッチ化の最も重要な例の1つとして、データソースとしてシステムコール（syscalls）を使用する場合が挙げられます。システムコールはあらゆるアプリケーションに不可欠であるため、あらゆる場面で発生します。システムコールから直接提供されるデータは、それを取り巻くコンテキストがなければ価値がないため、システムコールを取り巻くデータを収集して関連付けることが不可欠となります。

ホストエンドポイントに対するマイニング攻撃の場合、オペレーティングシステム（OS）固有のコンテキストを検知に含めることが望まれます。プロセスやスレッド、ファイルディスクリプタ、ユーザー、グループなどの情報は、すべてFalcoのデータリッチ化エンジンを通じて分析できます。この一連の情報は、ルール作成者がシステムコールイベントを有用なものにすることを可能にするような、基本的なメタデータを表しています。クリプトマイニングバイナリのルールにおいて、数値のファイルディスクリプタを使うことを考えてみてください。それよりも、「xmrig」のようなファイル名を使う方がずっと便利です。

Sysdigがもたらすメリット：Sysdigは、Falcoの機能を拡張および強化することにより、サーバー、コンテナ、Kubernetes、およびクラウドログのランタイムセキュリティに重点を置いたスケーラブルで包括的なセキュリティプラットフォームを提供しています。また、Sysdigの脅威リサーチチームは、特別に作成、最適化、キュレーションが施されたFalcoルールを自動的に提供することで、運用ワークフローを容易にしています。さらに、インタラクティブイベントや作成されたキャプチャから得た情報に基づくフォレンジックアクティビティ分析を通じて、調査と対応を強化しています。

コンテナ & Kubernetes

クラウド環境ではコンテナ化が一般的になっていますが、コンテナ化は独自のセキュリティ上の考慮点をもたらします。コンテナを標的とした攻撃は、コンテナのランタイムにおける脆弱性、設定ミス、またはセキュアでないコンテナイメージを悪用しようとします。イメージスキャン、ランタイム保護、振る舞い分析などを含む、コンテナセキュリティのための多層的な検知メカニズムを利用することで、悪意ある活動の特定とブロックやコンテナベースの攻撃の検知が行えるようになるほか、コンテナへのワークロード攻撃に関するリスクを軽減するためのセキュリティポリシーを実施できるようになります。

クラウドにおける設定ミスは、一般に、オンプレミス資産で想定されるよりも重大度の高い問題です。これは、境界線がないことが原因です。オンプレミス資産で設定ミスが発生した場合、一般的に、それらは組織のネットワーク内における特定のシステムまたはサーバーに影響を与えます。このような設定ミスでも重大な結果をもたらす可能性はありますが、多くの場合、それらはネットワーク境界内に収まります。一方、クラウド環境では、コンテナ化されたワークロードなどのインフラに対してセルフサービス機能が提供されることが多く、リソースの迅速なプロビジョニングと構成が可能になっています。このような俊敏性は有益ですが、一方で設定ミスの可能性が高まることもあります。適切な制御がなければ、設定時のミスや見落としが重大な結果をもたらす可能性があります。

Kubernetesは、コンテナ管理とスケーラビリティを簡素化するためのいくつかのコンセプトを導入しているものの、従来のセキュリティツールを使ったコンテナのセキュリティ確保はより困難になってきています。KubernetesがPod、サービス、デプロイメント、名前空間などの豊富な抽象化セットを提供し、ワークロード管理を合理化していることは、今や誰もが知っています。しかし、包括的なコンテキストを得るには、通常、Kubernetes Auditロギングサービスに接続する必要があります。

Falcoを導入した場合、クラスター内の各ノードはFalcoセンサーを実行します。起動時に、これらのセンサーはAPI Serverに接続してクラスターデータを収集し、初期のローカル状態を確立します。ホストOSからのデータリッチ化と同様に、Falcoはコンテナに比類のないコンテキストを提供するためにログデータを強化します。これにより、ユーザーはコンテナIDが生きている間に実行されたプロセスを確認できるようになるほか、それがどのPod、どの名前空間、およびどのデプロイメントに関連していたかを、Podの生死にかかわらず知ることができます。

また、クラウドネイティブ環境の動的な性質と、クラウド環境に引き継がれるレガシーなプラクティスを考慮すると、チームはしばしば「不変性（immutability）」に関するベストプラクティスを怠りがちであり、特に大規模環境ではドリフトに目をつぶってしまいかちです。「不変性」というワードを初めて耳にされた方は、「不変性」の原則とはクラウドネイティブ環境に固有のものであり、それは多くの場合セキュリティチームにとって有利に働くものであることを覚えておいてください。不変性とは、コンテナがライフサイクルを通じて変更されないことを保証するものであり、アップデート、パッチ、構成変更の必要性を排除するものです。

Kubernetesのような環境の場合、コンテナをキルすることは、Virtual Machinesのようなその他の仮想インフラをキルすることとは異なります。コンテナ型ワークロードはエフェメラル（短命）な性質があるため、Podがキルされると、まったく新しいPodにまったく新しいコンテナが作成されます。不変性の原理により、毎回同じ状態が再び作成されます。実行中のコンテナ内で変化が起きると、それはドリフトとみなされ、攻撃の兆候である可能性があります。

コンテナ内で起きたドリフトアクティビティを正確に追跡し、それをデータのリッチ化を通じてKubernetesレイヤーのコンテキストと相互に関連付けることができれば、どのようなセキュリティインシデントが発生し、どのKubernetes名前空間にそのインシデントが存在したかを知ることができます。

Sysdigがもたらすメリット： Sysdig Secureは、コンテナに関する脅威をリアルタイムで防止および検知した上で、それに対応することができます。SysdigのDrift Controlはさらに一歩進んで、新たに検知された実行可能ファイルをブロックして、実行できないようにします。このようなプロアクティブな対策を利用することで、実行時に悪意あるコードが実行されるリスクを回避できます。

サーバーレス

サーバーレスコンピューティングは、基盤となるインフラやコード実行環境に対する潜在的なリスクなど、独自のセキュリティ課題をもたらします。サーバーレス環境に対する攻撃は、サーバーレス機能の操作、不正なアクションの実行、機能のコードに含まれている脆弱性の悪用などを試みる可能性があります。

コード分析、振る舞いの監視、異常検知などを含む、サーバーレスセキュリティのための多層的な検知メカニズムを利用すると、サーバーレス環境に対するワークロード攻撃を特定した上でそれに対応することができるようになり、サーバーレスアプリケーションの整合性とセキュリティを確保できます。

クラウドプラットフォームの進化に伴い、利便性と抽象度の両方が同時に高まっており、新しいエージェントモデルが求められています。

たとえば、AmazonのECSやEKSの場合、ユーザーは基盤となる仮想ホストマシンを管理する責任があります。しかし、Fargateのような環境では、ホストはクラウドプロバイダーによって暗黙のうちに割り当てられ、ユーザーはその下のコンピュートインフラの割り当てや設定をすることなく、または何の知識も持たずにコンテナを実行するだけです。

このような「Container-as-a-Service」モデルは便利ですが、それはリスクをもたらす可能性があります。多くのユーザーがコンテナを放置し、コンテナ内部のセキュリティイベントを監視しないことが原因で、シークレットの流出やビジネスデータの漏洩が発生し、アマゾン ウェブ サービス（AWS）/クラウドプロバイダーのコストが増大する可能性があります。

残念ながら、ほとんどの従来のEndpoint Detection & Response（EDR）ツールにとって、ホストへのアクセスがなければ、ワークロードのアクティビティに対する可視性は、サーバーレス環境では制限されることがあります。これらの理由から、FalcoのようなプロジェクトがAWS Fargateと連携するようなインスツルメンテーションを構築することは理にかなっています。

実際、SysdigによるFalcoの導入は、現時点で、一元管理が可能なAWS Fargateオーケストレーターエージェントを提供する唯一のソリューションです。このエージェントは、AWS Fargateタスクの保護に必要となる深いレベルの可視性を提供する特定のAWS Fargateタスクとの間のすべてのポリシー、接続、イベントを効果的に管理するために必要となるものです。

Sysdigがもたらすメリット：Sysdigのサーバーレスワークロードエージェントは、各Fargateタスクにインストールされます。それは、サーバーレスワークロードを監視し、Falcoのポリシーとルールを適用することで、セキュリティ脅威の検知を行います。

クラウドサービス

クラウドの設定ミスは、クラウド環境における最も一般的なセキュリティリスクの1つです。攻撃者は、不正アクセスや機密データの取得のために、誤って設定されたアクセス制御、弱い認証メカニズム、不適切に管理されたストレージリソースを狙うことがよくあります。多層的な検知は、構成監視、脆弱性スキャン、ポリシー実施などのさまざまなメカニズムを採用することで、これらの設定ミスを特定し、それらがもたらすリスクを軽減します。

イベントデータの収集方法については、通常、次のようなアーキテクチャーに関する2つの選択肢があります。

1. クラウドAPIを照会するか、クラウドデータストアを監視することで、設定ミスを検知します。
2. クラウドのログをバックエンドにストリーミングして、ログのインデックスを作成し、ユーザーがログを照会できるようにします。

脅威をリアルタイムで検知することを意図している場合、最初のオプションでは十分ではありません。ポーリングの唯一の利点は、コンプライアンスレポートや検証チェックを行う必要がある場合です。この種の動作は間違いなく一定の間隔で実行できますが、これは、脅威をできるだけ早く検知/停止する必要があるインシデントレスポンスチームのリアルタイム性を無視したものです。

2つ目のアプローチは、SIEMソリューションと同じものです。SIEMは可能な限りすべてのイベントを取り込む傾向があり、関連するアラートを発行するためにこれらのイベントを収集できるような膨大なストレージを必要とします。関連するクラウドAPIを照会するというポーリングオプションは、確かにSIEMソリューションよりも少ない量のストレージで済みますが、アラートのリアルタイム性に欠けるのも事実です。これが、Falcoが本番システムにおける完璧な妥協点となっている理由です。

上記以外のFalcoのアプローチは、リアルタイムのイベントストリーミングに通常ありがちな煩雑なオーバーヘッドを伴わずに、リアルタイムの脅威を検知する効果的な方法を提供します。Falcoは、リアルタイムで脅威を検知するためにストリーミング方式でデータを解析し、実行とデプロイが驚くほど軽量なエンジン上に検知を実装します。さらに、Falcoは、柔軟で表現力のあるコンパクトなルール言語を提供します。Falcoはリソースをほとんど消費しませんが、最も重要なことは、それがストリーミング方式でデータを分析することです。コストの高いコピーを実行する必要はなく、データがインデックス化されるまで待機する必要もありません。

Sysdigがもたらすメリット： Sysdigは、エージェントレスとエージェントベースの両方のアプローチを取り入れることで、初期導入の容易さとスピードだけでなく、セキュリティチームがクラウドセキュリティを確立するプロセスを進める中で、深い可視性とより強固なセキュリティへの要求との間でバランスを取っています。エージェントベースとエージェントレスによる検知の利点の詳細については、当社のホワイトペーパー「dedicated to the topic」をご覧ください。

アイデンティティ

アイデンティティに基づく脅威は、クラウド環境内のユーザーアカウント、認証情報、または特権への不正アクセス、誤用、またはハッキングを伴います。IDベースの脅威を検知するための多層的な検知メカニズムには、ユーザー行動分析、クラウドログの分析による異常検知、およびIAMログ（Oktaなど）が含まれます。これらのメカニズムは、疑わしい活動の特定、ハッキングされたアカウントの検知、不正アクセスや内部脅威を防ぐためのアクセス制御の実行に役立ちます。

2022年3月、LAPSUS$というサイバー犯罪者集団が、15,000社以上の企業に広く利用されているIDプラットフォームであるOktaへのハッキングに成功したと主張しました。このセキュリティ侵害は発表のわずか2カ月前に発生し、Oktaの顧客は自分たちの機密データも侵害されたのかどうかわからないままでした。このセキュリティインシデントの結果、Oktaのセキュリティチームは徹底的な調査を行った後、同攻撃に関するいくつかの詳細を発表しました。

OktaのIDサービスは、組織内のネットワークやリソースに、許可された個人だけがアクセスできるようにするためのものです。この種のサービスは、金融機関や医療機関など、機密情報を扱う企業にとって特に重要です。しかし、今回のセキュリティ侵害は、組織内で不審な行動が発生した場合に、それをいち早く検知することの重要性を改めて浮き彫りにしました。

早期発見により、企業は、データ窃取、金銭的損失、風評被害など、サイバー攻撃により引き起こされる潜在的な損害を軽減できます。企業は、高度化するサイバー脅威からシステムとデータを守るために、強固なサイバーセキュリティ対策に投資することが不可欠です。

従来のクラウドセキュリティポスチャー管理（CSPM）ソリューションは、スケジュールされた間隔でレポートを作成するため、すでに被害が発生した後でないと、レートリミットの問題を検知できない可能性があります。このアプローチは、認証システムに対するリアルタイムの可視性を提供しないため、レートリミットの問題に対処する際には有用ではありません。その結果、セキュリティチームは、侵害につながりかねない重要なセキュリティイベントを見逃す可能性があります。

OktaのようなFalcoプラグインの場合、Falcoで使用されているその他のプラグインやコアライブラリによって提供されていたイベントに対して、追加のフィールド抽出機能を提供するものです。平たく言えば、これによりFalcoはデータソースフィールドの値を返すロジックを実装できるため、さらに充実したメタデータを提供できます。これにより、インシデント対応者は、Oktaのイベントをリアルタイムのクラウド、コンテナ、ホストのアクティビティと組み合わせることで、ハッキングされたユーザーからクラウドネイティブなワークロードにおける影響まで、攻撃全体をよりよく理解できるようになりました。

Sysdigがもたらすメリット：Sysdigは、実行時のアクセスパターンの分析に基づいて過剰な権限を優先順位付けし、削減できます。また、Sysdigは、新しいSysdig Okta検知機能により、MFA疲労攻撃（スパム）やアカウント乗っ取り（ATO）などのID攻撃を検知するほか、Oktaイベントをリアルタイムのクラウドやコンテナアクティビティとつなぎ合わせることで、ユーザーから影響に至るまでの攻撃全体をチームが把握できるようにします。

サプライチェーン

近年、サプライチェーン攻撃が大きな問題となっています。これは、開発、配布、導入の過程で信頼できるコンポーネントやソフトウェアを攻撃者がハッキングするものです。この攻撃は、悪意あるコード、バックドア、または脆弱性をクラウドシステムに導入する可能性があります。サプライチェーン攻撃を特定し、それがもたらすリスクを軽減するには、多層的な検知メカニズムが不可欠です。このメカニズムは、ソフトウェアやコンポーネントの完全性を分析し、コード解析を行い、脅威インテリジェンスを活用することで、サプライチェーンの侵害を検知し対応するものです。

しかし、多くの組織は、ソースコードリポジトリを保護するための基本的なセキュリティ対策を実施できていません。たとえば、リポジトリへのアクセスを許可された担当者のみに制限していなかったり、アカウントを保護するために2要素認証を使用していなかったりすることがあります。さらに、企業や組織の中には、秘密鍵などの機密情報が公開リポジトリにプッシュされるリスクや、プライベートリポジトリが誤って公開リポジトリに変更されるリスクを見落とすものもあります。このような見落としがあると、データ漏洩やサイバー攻撃に対して脆弱なままになってしまいます。

よくある問題として、企業はGitHubリポジトリを含む包括的なセキュリティ計画を策定していない可能性があります。ソースコードリポジトリのリスクや脆弱性は急速に変化する可能性があり、企業はサイバー攻撃の犠牲者にならないよう、このような変化に対応する必要があります。ここで、専門の脅威リサーチチームが、ネット上の最新の脅威を特定し、GitHubの悪意のある行動を検知するためのセキュリティルールを更新するという重要な役割を果たすことができるのです。

チームのGitHubリポジトリのセキュリティを確保することは最重要ですが、その最も重要な側面の1つは、CI/CDパイプラインにおけるシークレットの露出を検知し、防止することです。パスワード、トークン、APIキーなどのシークレットを公開すると、ハッカーが機密データに不正にアクセスできるようになり、致命的な結果を招くことがあります。

公開リポジトリでのシークレット漏洩は明らかな懸念事項ですが、プライベートリポジトリも同様に攻撃されやすいものです。プライベートリポジトリのシークレットを悪用すると、権限昇格やラテラルムーブメントにつながり、チームのセキュリティに重大なリスクをもたらす可能性があります。ここで実証されているように、大手自動車メーカーが「秘密鍵」を公開するという単純なミスを犯した結果、重大なデータ漏洩につながったというケースもあります。

残念ながら、シークレット漏洩の検知と防止は、特に大規模なチームでは困難な場合があります。各メンバーのgitへのアクセス方法やコミット内容を管理するのは難しく、AWSのgit-secretsのようなツールを使ったとしても、効果を上げるにはそれをすべてのクライアントにインストールすることが不可欠です。さらに、シークレットを削除したとしても、それがリポジトリの履歴に残ってしまうため、完全な削除は不可能です。

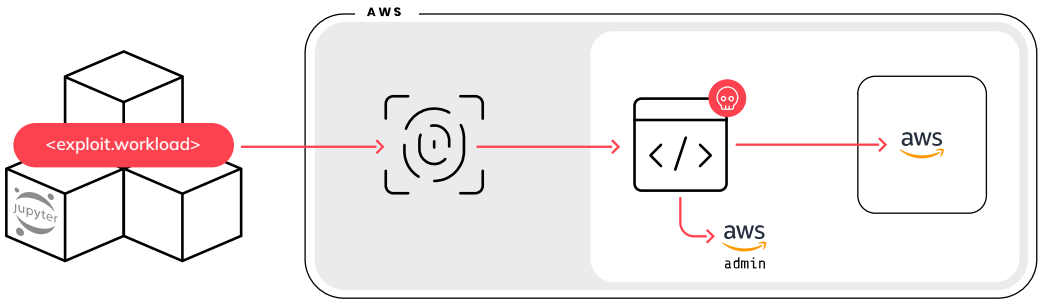
Sysdigがもたらすメリット：Sysdigは、実行時のアクセスパターンの分析に基づいて過剰な権限を優先順位付けし、削減できます。また、Sysdigは、新しいSysdig Okta検知機能により、MFA疲労攻撃（スパム）やアカウント乗っ取り（ATO）などのID攻撃を検知するほか、Oktaイベントをリアルタイムのクラウドやコンテナアクティビティとつなぎ合わせることで、ユーザーから影響に至るまでの攻撃全体をチームが把握できるようにします。

実際のサイバー攻撃の事例：SCARLETEEL攻撃のステップごとの説明

攻撃ステップ1：コンテナ経由のデータ流出

Sysdigの脅威リサーチチームは、最近、SCARLETEELと名付けられた巧妙なクラウド攻撃を発見しました。この攻撃者は、コンテナ化されたワークロードを悪用し、それを利用してAWSアカウントへの権限昇格を実行することにより、プロプライエタリなソフトウェアと認証情報を盗み出しました。

この攻撃は、その他多くの攻撃に比べて、より巧妙なものでした。それは、Kubernetesコンテナのハッキングから始まり、被害者のAWSアカウントへと広がったため、コンテナ、Kubernetes、クラウドからのコンテキストのリッチ化を通じたエンドツーエンド検知の現実的な必要性を浮き彫りにしました。SCARLETEEL攻撃において、攻撃者は、Kubernetesクラスター内に導入されたインターネット公開型のWebアプリケーション（サービス）を見つけて悪用しました。攻撃者はコンテナにアクセスした後、攻撃を進めるためにさまざまなアクションを実行し始めました。



攻撃ステップ2：ホストとコンテナにおけるマイニング検知

上の図からわかるように、この攻撃の目的は、Webアプリケーションを悪用してクリプトマイニングを実行することをはるかに超えたものでした。クリプトマイニングは事実上すべての環境（コンテナ、ホスト、サーバーレス）でよく知られた脅威であるため、攻撃者がマイニング活動を囮にして、プロプライエタリなデータの流出など、価値の高い活動の検知を回避する可能性は十分あります。

攻撃ステップ3：クラウドにおける防御回避

SCARLETEELの攻撃者は、S3バケットとLambda関数から機密性の高い認証情報にアクセスすることができ、それによりラテラルムーブメントを実行できました。私たちはAWS Cloudtrailログ内でこのすべての活動を追跡することができますが、攻撃者が検知を回避するためにCloudtrail監査サービスを無効にしようとした場合はどうなるでしょうか？ありがたいことに、SysdigとFalcoは、CloudTrailのログを無効にするような、クラウドにおける疑わしいユーザーの活動を検知できます。コンテナ、ホスト、Kubernetes、クラウドからのデータをリッチ化することで、私たちは、コンテキストを伴う攻撃の全体像を明らかにすることができます。

攻撃ステップ4：IDプロバイダーにおける認証ログインの失敗

SCARLETEEL攻撃では明示されていませんが、多くの攻撃者は、内部インフラにアクセスするために、追加の認証制御を迂回しています。そのため、ユーザーがレートリミット（たとえばOKTAリクエストなどに関するもの）に達しているかどうかを検知することも重要です。これは、組織のリソースのセキュリティに対する潜在的な脅威を示す可能性があります。攻撃者は、ブルートフォース攻撃を使ってパスワードを推測するか、または大量のリクエストで認証システムを圧倒することで不正アクセスを行う可能性があります。エンドツーエンドのセキュリティの観点からは、クラウドを保護するツールのアクティビティをリアルタイムで検知する必要もあります。

攻撃ステップ5：サプライチェーンにおける機密性の高い認証情報の公開

SCARLETEEL攻撃で見られたように、Terraformの状態ファイルにはすべてのデータがプレーンテキストで含まれており、これにはシークレットを含んでいる可能性があります。セキュアな場所以外にシークレットを保存することは決して良い考えとは言えませんし、シークレットは絶対にソース管理システム内に置いてはなりません。これと同じロジックをシフトレフトの方法論全体に適用する必要があります。機密性の高い認証情報が誤ってGithubリポジトリにコミットされた場合、そのことをどうやって知るのでしょうか？同僚がこの安全でないコミットを知らせてくれるのを待つのでしょうか？もしそうなら、コミットしてからどれくらいの時間でそのことに気付くのでしょうか？セキュアでない場所に誤って公開された機密データに脅威アクターがアクセスできないようにするためには、サプライチェーンからコンテナワークロードに至るまで、リアルタイムの検知を実施する必要があります。

結論

市場の観点からは、ホストやコンテナにおける単なるシステムコールの検知にとどまらないことが必須となります。進化し続けるクラウドベースの脅威から効果的に身を守るためには、Kubernetesから抽出された情報、クラウド監査ログ、ソースリポジトリ、IDプロバイダーのコンテキストを取り込むことによって、データを強化することが不可欠となります。スタック全体でリアルタイムに脅威を検知してそれに対応するためには、複数のソースからのログの取り込みが不可欠となります。

今日の市場環境では、複雑で高度な攻撃には、スタック全体をカバーする包括的な検知機能が必要です。たとえば、SCARLETEELのようなサイバー攻撃では、さまざまなソースからログを取り込むだけでは十分ではありませんでした。リソースのオーバーヘッドを最小限に抑えつつ高いスケーラビリティを実現するためには、制限された状態を維持しつつ、中央集権型のストレージを避けることが不可欠となります。Falcoに代表されるように、クラウドの検知と対応における真にスケーラブルな唯一のアプローチとは、ルール評価を水平に分散させることであり、これによりスケーラブルで効果的なソリューションを保証できます。

クラウド脅威を検知するための Falcoの役割

CNCFの最近の卒業プロジェクトであるFalcoは、ホスト、コンテナ、Kubernetes、クラウドのランタイムセキュリティのためのオープンソースセキュリティソリューションです。Falcoは、包括的な脅威対策のためのコアエンジンとして機能します。エンドツーエンドの検知機能は、リアルタイム検知、多層コンテキスト、カスタマイズ性、活発なコミュニティとエコシステム、そして拡張性を包含しています。これらの側面に関する詳細な説明を下記に示します。

1. **リアルタイム検知：** Falcoのアーキテクチャーは、遅延と追加コストが発生するような従来の後処理手法には頼らず、データのリアルタイムストリーム処理を実行する点でユニークです。そのeBPFを搭載したインスツルメンテーションは、すべてのクラウドワークロード（VM、コンテナ、サーバーレスなど）のすべてのシステムコールに対して深いリアルタイム可視性を提供し、平均して5分未満の短命なコンテナ内のものであっても脅威を検知します。
2. **多層的なコンテキスト：** Falcoは、コンテナランタイム（例：Docker）、オーケストレーター（例：Kubernetes）、クラウドプロバイダーのメタデータ、アイデンティティプロバイダー（例：Otka）など、さまざまなソースに由来するディープなコンテキストを収集することで、検知をリッチ化します。
3. **カスタマイズ性：Falcoは高度なカスタマイズが可能であり、ユーザーはそれぞれのニーズや環境に合わせたカスタマイズが行えます。Falcoは、企業や組織に固有の脅威状況に関連する特定の行動や活動を検知し、警告するように構成できます。この柔軟性により、脅威状況の進化に応じて検知能力を適応させ、それを改良できます。**
4. **活発なコミュニティとエコシステム：** Falcoは、多様なコミュニティの集合知と専門知識から恩恵を受けており、より幅広いユースケース、統合（プラグインなど）、およびベストプラクティスを提供します。この活発なコミュニティは、Falcoが常に最新であり、新たな脅威に対応できることを保証します。
5. **拡張性：** Falcoのプラグインアーキテクチャーは、ユーザーが追加の機能を開発し、Falcoのランタイムに統合することを可能にすることで、拡張性とカスタマイズ性を実現します。この結果、Falcoの機能を強化し、新しいルールを導入し、外部システム（クラウド、アイデンティティ、サプライチェーン、サードパーティアプリのログなど）と統合できるプラグインを作成するためのフレームワークを提供できます。

Falcoが最高のエンドツーエンド検知アプローチを提供できるのには、いくつかの理由があります。Falcoは、あらゆるワークロード、クラウド、サービスにわたる幅広さを提供しており、これにより、クラウドインフラに関係なく一貫した脅威の検知と可視性を維持することができます。また、Falcoは、機械学習（ML）、ルール、脅威フィードなど、さまざまな技術を組み合わせることで得られる底深さを提供しており、これにより脅威を効果的に検知して対応することが可能となります。

このような「幅広さ」と「底深さ」の組み合わせにより、疑わしい活動を特定する精度を向上させ、企業のクラウド環境における既知の脅威と新たな脅威の両方に対する強固な防御を提供することが可能となります。Sysdigは、Falcoを開発した後、Cloud Native Computing Foundationへの寄贈を通じてFalcoを一般に公開しました。Sysdigは、Falcoを包括的なCNAPPプラットフォームの中核に据えています。

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。

デモを依頼 →

sysdig

ホワイトペーパー

WP-008-JA REV. B 9/24