sysdig | aws

ランタイムインサイトとセキュリティデータレイクにより大規模環境でのイノベーションを実現

Sysdig SecureとAmazon Security Lakeを組み合わせることで、クラウド資産を保護するための最新の基盤を提供

目次

最新のクラウド環境には、大規模環境での合理化されたセキュリティが必要

クラウドネイティブアプリケーションとインフラストラクチャーの規模が拡大するにつれ、セキュリティチームはマルチクラウドやハイブリッド環境全体でセキュリティを管理し高速化するための、効果的な方法を必要としています。コンテナ、Kubernetes、クラウドサービスはデジタルトランスフォーメーションを推進していますが、アマゾン ウェブ サービス（AWS）上の構築スピードに後れずについていけるような、堅牢なセキュリティを確保することは困難です。

セキュリティチームは、状況を明確にし、脅威をリアルタイムで検知し、対策を講じることを可能にするソリューションを必要としています。このようなソリューションを利用することで、セキュリティチームはリスク管理を強化し、不正アクセスを防止できるようなります。

Sysdig SecureとAmazon Security Lakeを組み合わせることで、クラウド資産を保護するための最新基盤を提供できます。

Sysdig Secureの、Amazon Security Lakeとの統合で、大規模環境におけるセキュリティとコンプライアンスへの効率的で合理化されたアプローチを構築できます。

下記では、これら2つのソリューションを使ってどのようにセキュリティデータを管理し、より正確な分析と効果的な保護が可能になるかを紹介します。

クラウドで構築する際のセキュリティ上の課題

セキュリティデータは、データ、アプリケーション、ワークロード、環境を保護するために不可欠です。しかし、次のような課題が、プロセスと精度を妨げています。

動的な環境における可視性のギャップ：開発者は、インフラを意のままに構成しており、ボタンをクリックするだけでコンテナ化されたマイクロサービスを導入しています。このため、大量のクラウド資産を追跡し、IAM権限を管理することが必要となっています。

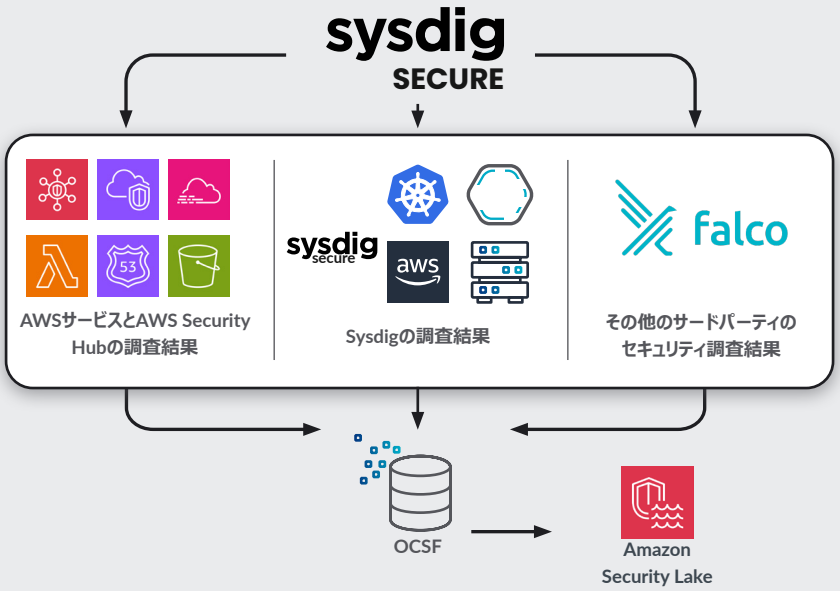
増大するセキュリティデータ：クラウド環境が拡大し続ける中、セキュリティチームは、データの分析よりもデータ管理に多くの時間を費やしています。つまり、大量のアラートの中で、優先度の高い脅威に対処することが困難になっています。

サイロ化したソリューションと一貫性のないデータ：多くの場合、異種のセキュリティツールは相互に通信を行わず、コンテキストを共有することもありません。ログやアラートの形式はさまざまであり、それらは見つけるのが困難なサイロに存在することもあります。

リアルタイム検知と専用のデータレイクの組み合わせ

Sysdigが持つ強力なランタイムセキュリティ機能と、スケーラブルで費用対効果の高いデータレイクソリューションを組み合わせることで、組織全体におけるセキュリティデータのより包括的なビューを確保できるようになります。SysdigとAmazon Security Lakeの統合により、AWS上で、リッチ化されたマルチプラットフォーム型のクラウドセキュリティイベントを保存できるようになり、お好みのアナリティクスツールを使用してセキュリティデータを分析できるようになります。

Amazon Security Lakeは、ログとセキュリティ上の発見を自動的に収集し、Open Cybersecurity Schema Framework（OCSF）を使用して、それらのデータを同じフォーマットで整列させます。OCSFのサポートにより、Amazon Security Lakeは、入力されたログデータをパーティショニングした上で、それらをストレージ効率とクエリ効率の高い形式へと変換します。その結果、お客様は、データを後処理することなく、直ちに幅広く使用して、セキュリティアナリティクスを行えるようになります。



SysdigのCNAPPによりランタイム保護を実現：Sysdig Secureは、ランタイムインサイトを使用したCloud-Native Application Protection Platform（CNAPP）であり、クラウドチームとセキュリティチームは、これを使うことにより、リアルタイムで脅威を検知して対応できるようになります。

Amazon Security Lakeによりデータを一元化：Amazon Security Lakeは、AWS環境、SaaSプロバイダー、およびオンプレミスのソースから収集したセキュリティデータを、お客様のAWSアカウントに保存されているデータレイク内で一元管理できるようにする専用サービスです。

Open Source Foundationに基づいて構築

Sysdigは、クラウド脅威検知のためのオープンソースソリューションであるFalcoの開発元です。Falcoはオープンソースであるため、標準化を推進し、コミュニティによる貢献でイノベーションを加速するのに役立ちます。

OCSFもオープンソースのプロジェクトであり、セキュリティデータに関する簡素化されたベンダー非依存の分類法を提供します。OCSFは、あらゆる環境、アプリケーション、ソリューションプロバイダーで採用できます。

クラウドを
エンドツーエンドで保護

Sysdig Secureは、リアルタイムの振る舞いに関するインサイトと脅威インテリジェンスを活用することで、インフラストラクチャーとアプリケーションを継続的に監視し、絶えず進化し続ける脅威に対する統合的かつプロアクティブな防御を実現します。ランタイムインテリジェンスのパワーを利用することで、お客様は、Amazon Elastic Kubernetes Service（Amazon EKS）、Amazon Elastic Container Service（Amazon ECS）、AWS Fargateなどのクラウド環境全体における脅威を特定し、それらの脅威に即座に対応するために必要となるインサイトを得ることが可能となります。

セキュリティイベントや不審な活動の指標を自動的に取得し、Amazon Security Lakeに保存します。Sysdigの調査結果は、AWS CloudTrail、AWS Security Hub、Amazon Inspectorなどのような、その他のネイティブAWSサービスから収集したデータと共に利用できます。これらのサービスは、Amazon Security Lakeと統合されているため、複数のソースから収集したセキュリティ調査結果を簡単に統合できます。

Amazon Security LakeとSysdig Secureのリアルタイムインテリジェンスを活用することで、コードから対応に至るまで、お使いのAWS環境を包括的に保護できます。

コード	ビルド	実行		対応
Infrastructure as code (IaC) の検証	**脆弱性管理**	**設定と権限の管理**	**脅威の検知**	**インシデント対応**
危険な設定をブロック	CI/CDとレジストリでのスキャン	クラウドの設定ミスを検知	MLとFalcoを使用して多層的な検知を実現（脅威、ドリフト、クリプトジャッキングなど）	フォレンジックのための詳細な記録の取得
ソースレベルでの自動修正	リスクのあるイメージをブロック	最小権限アクセスを実施		設定に関する問題を修正
	ランタイムコンテキストを使用した脆弱性の優先順位付け	OPAを使用して一貫性のあるポリシーを適用	K8sによるネイティブマイクロセグメンテーションを実装	悪意ある活動をブロック

価値あるユーケースの宝庫

Amazon Security Lakeは、Sysdigのセキュリティインサイトを利用するために、数多くのユースケースをサポートしています。そのトップ3を下記に示します。

セキュリティ調査を合理化： Sysdigを使用して脅威を調査することや、Amazon Security Lakeおよびその他のお好みのアナリティクスツールを使用してセキュリティデータを分析することにより、潜在的なセキュリティ問題に関するインサイトを明らかにします。セキュリティ関連のログと調査結果を同じ形式で一元管理することで、セキュリティチームは、より広範な可視性を持てるようになり、徹底的な調査と迅速な対応が行えるようになります。

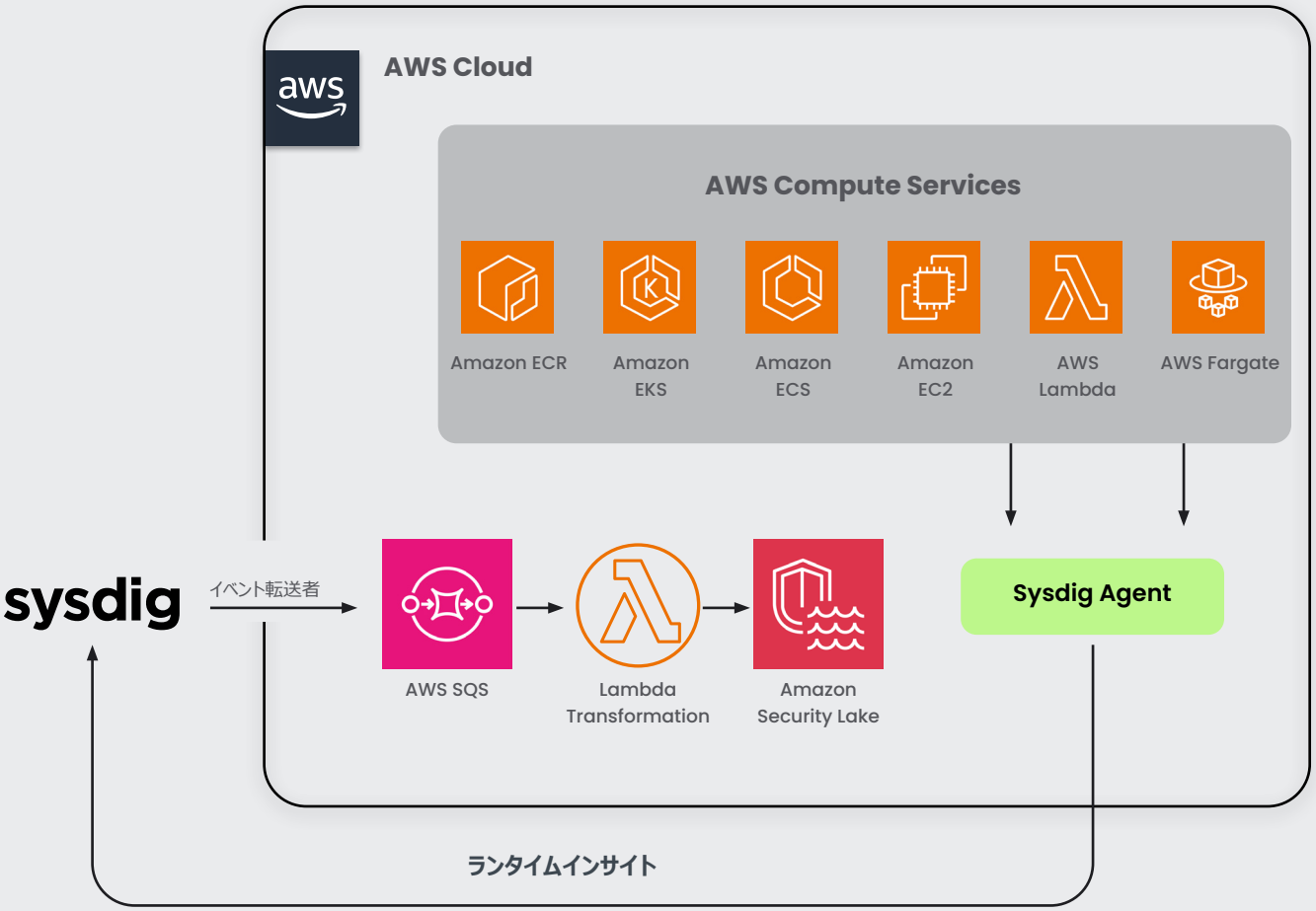
セキュリティ監視を最大限に強化： SysdigのランタイムインサイトとAmazon Security Lakeによる大規模環境でのデータ管理により、ビジネス全体のリスクをより包括的に把握できるようになります。Amazon Security Lakeは、Sysdig、AWS、サードパーティのツール、オンプレミスのソリューションからペタバイト単位のデータを一元管理します。また、セキュリティ情報イベント管理（SIEM）や拡張検知対応（XDR）ツール、Amazon AthenaやAmazon OpenSearch Serviceのような一般的なデータアナリティクスサービスと統合することで、大量のデータを迅速に照会し分析できるようになります。

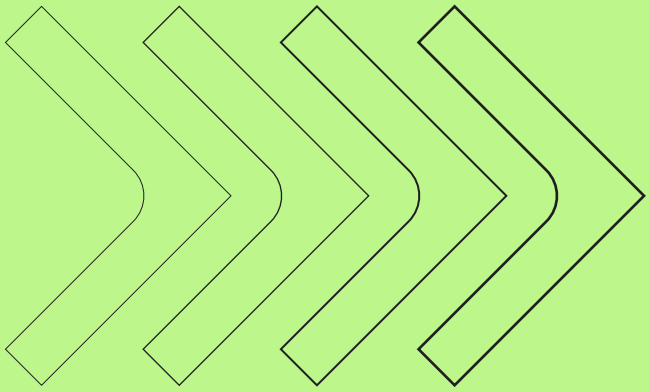
クラウドコンプライアンスを簡素化： SysdigとAmazon Security Lakeを使うと、複数のリージョンやアカウントにまたがるコンプライアンスの測定、監視、報告が簡単に行えるようになるため、情報収集や証明に費やす時間を削減できます。さらに、複数のログソース、AWSリージョン、アカウントからのセキュリティデータを1つまたは複数のロールアップリージョンに一元化することで、コンプライアンスとレポーティングに関する義務を簡素化できます。また、カスタマイズ可能な保持設定により、特定の期間データを保存するような規制上の義務にも対応できます。

Amazon Security Lakeに
イベントを自動送信

Sysdig Secureは、オープンソースのFalcoに基づく検知ルールを使用して、アプリケーションとインフラストラクチャー全体でリアルタイムにランタイムイベントをキャプチャします。あるアクティビティが疑わしく見える場合や、またはそれが侵害の痕跡と一致する場合、アラートがトリガされます。当該イベントの詳細は、地域、ユーザー、ネームスペースなどのコンテキストと共にキャプチャされ、調査に利用されます。

続いて、Sysdig Secureは、組み込みのイベント転送機能を使用して、セキュリティイベントをAmazon Simple Queue Service（Amazon SQS）へと自動的に送信します。Sysdig Secureのインターフェイスを使用して、AWS CloudFormationテンプレートまたはTerraformテンプレートを導入し、Amazon SQSとLambda関数を作成できます。AWS Lambda関数がトリガされると、抽出、変換、ロード（ETL）変換が開始され、実行時の調査結果がOCSF形式でAmazon Security Lakeにバッチでアップロードされます。





sysdig | aws

ご自分の目で確かめよう

SysdigがAWSクラウド上でいかにイノベーションを確保しているかについてはこちらを、AWS MarketplaceでのSysdigソリューションはこちらを、Sysdig Secureを使い始める方法についてはこちらをご覧ください。