sysdig | aws

Sysdigイベントを Amazon Security Lakeへ転送

広範なクラウドネイティブセキュリティの世界では、自社のセキュリティデータを理解し分析することが最も重要です。お客様のシステムに詳細なランタイムインサイトを提供する包括的なセキュリティプラットフォームとして開発されたSysdigをAmazon Security Lakeと統合することで、セキュリティデータ分析のための強力な一元化されたプラットフォームを手に入れることができます。このガイドでは、SysdigとAmazon Security Lakeをシームレスに統合するための手順を紹介します。

目次

コンセプト

OCSF

オープンサイバーセキュリティスキーマフレームワーク（OCSF）は、オープンソースのコラボレーティブなスキーマフレームワークです。OCSFは多くのイベントタイプの標準スキーマを提供します。アマゾン ウェブ サービス（AWS）は、Amazon Security Lakeデータにおいて、このスキーマタイプを採用しています。詳細については、下記のリンクをご覧ください。

- オープンサイバーセキュリティスキーマフレームワーク（OCSF）
- OCSFスキーマ

Parquet

Parquetは、効率的な方法でフラットなカラム型のデータを格納するために使用される、オープンソースのファイルフォーマットです。これにより、クエリのパフォーマンスを最適化できます。

- Parquetのドキュメント

Sysdigイベント/ログ

Sysdigイベント転送機能を使うと、ポリシーイベント、Sysdigプラットフォーム監査、ベンチマーク（レガシー）、およびホストスキャンを送信できます。

ポリシーイベント
さまざまなポリシー/ルールに基づく、Sysdigのランタイムインサイトイベントです。

- イベント転送

Sysdigプラットフォーム監査
Sysdigプラットフォームのイベントであり、これにはポリシーの変更、ユーザーの追加、アラートの変更などが含まれます。

- Sysdigプラットフォーム監査

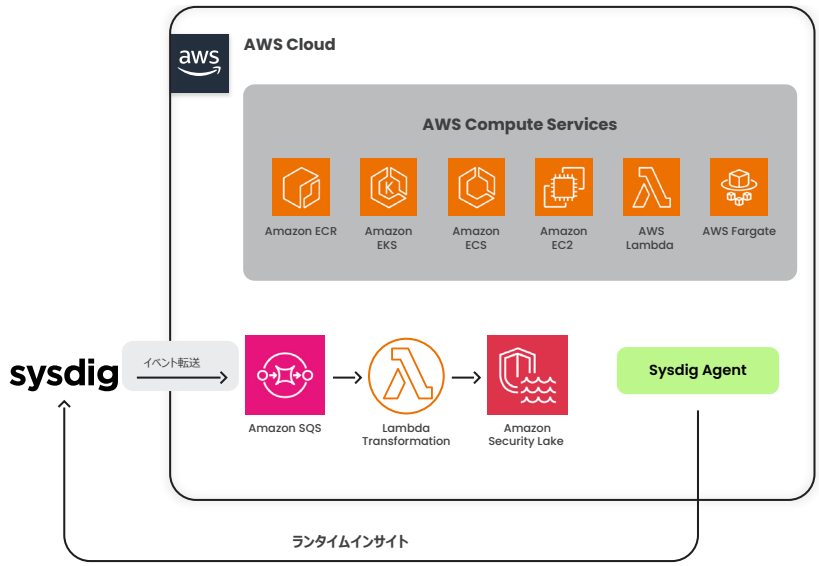
ベンチマーク（レガシー）
各種のコンプライアンスフレームワークに関連したドリフトイベントです。

- コンプライアンスのレガシーバージョン

ホストスキャン
ホスト脆弱性の自動スキャンおよび手動スキャンに関するイベントです。

- ホストスキャン

図1：
Sysdig Security Lake
アーキテクチャー



前提条件

- **AWSアカウント：**AWS Lambda、Amazon SQS、AWS CloudFormationの権限を持つロールが設定されているアカウントです（Amazon Security Lakeが有効化されているAWSアカウントが必要です。また、Amazon Security Lakeにイベントを転送させたいAWSアカウントへのアクセス権も必要となります）。
- **Sysdigアカウント：**イベント転送機能を持つアカウントです。
- **Sysdig外部ID：**Sysdig AWS CloudFormationのテンプレートを導入している場合、「AWS CloudFormation」パラメータタブで確認できます。そうでない場合は、Sysdig UIに移動し、Integrations → Cloud Accounts → Add an AWS single accountへと移動し、Launch stackをクリックして、外部IDを見つけます。
- **AWS IAMユーザー：**イベントの転送先とするAWSアカウントで作成されたAWS IAMユーザーであり、Amazon Security Lake用のSysdigイベントを保持するイベント転送キューへのAmazon SQS権限を持っています。
- **Amazon Security Lakeカスタムソース：**Sysdig外部IDを通じて構成されたカスタムソースです。
- **知識：**AWS Lambda、Amazon SQS、Amazon S3、AWS CloudFormationに関する基本的な知識が必要です。

Amazon Security LakeでSysdig用のカスタムソースを作成

Amazon Security Lakeは、AWSサービスと外部パートナーの両方からのイベントのためのランディングスポットです。Amazon Security Lakeはカスタムソースコンストラクトを使用して、パートナーがイベントを送信できるようにします。このためには、まずAmazon Security Lakeで、Sysdig用のカスタムソースを作成する必要があります。これにより、Amazon Security Lakeに必要なIAMロールとAmazon S3バケットの両方が作成されます。作成時に、Sysdig外部IDの入力を求められます。カスタムソースの作成に関する詳細は、下記をご覧ください。

- カスタムソースからのデータ収集

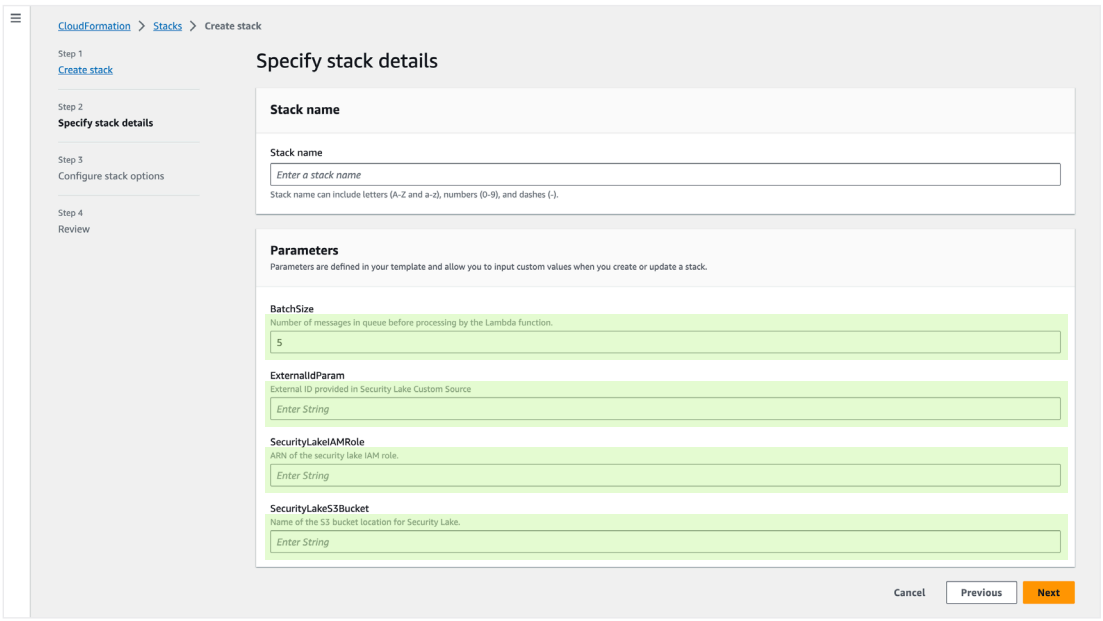
AWSリソースの導入

01

AWS CloudFormationスタックの導入：

1. AWS Consoleを通じてAWS CloudFormationにアクセスします。
2. 新しいスタック作成プロセスを開始します。
   a. Amazon SQSへのSysdigイベント転送機能をまだセットアップしていない場合（この場合、Sysdigイベント転送キュー/DLQと実行ロールを作成し、Lambda関数をトリガとして導入する必要があります）：
      - https://sysdig-securitylake-lambda.s3.amazonaws.com/SecurityLake.yaml
   b. Amazon SQSへのSysdigイベント転送機能を既にセットアップしている場合、下記のCloudFormationを導入した上で、Lambda関数をAmazon SQSトリガとして設定します（Amazon SQSキューを既にセットアップしており、かつSysdigからのイベント転送をセットアップしている場合は、この方法を使用します。これにより、トリガ用のLambda関数のみが導入されます）：
      - https://sysdig-securitylake-lambda.s3.amazonaws.com/SysdigSecurityLake.yaml

図2：
AWS CloudFormation
スタックパラメータ



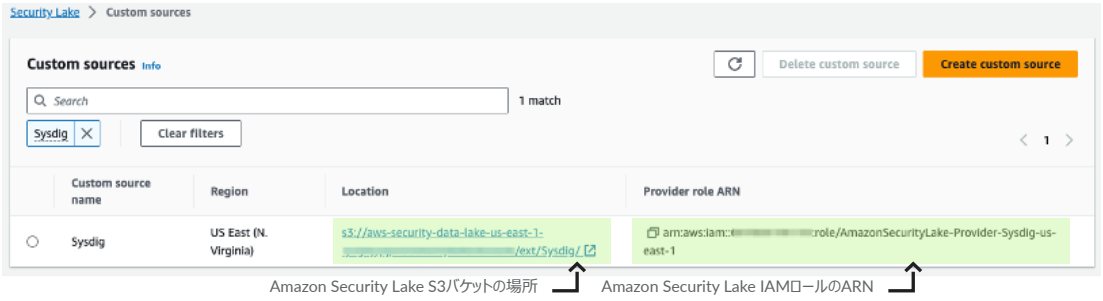
c. メッセージのバッチサイズを指定します。

d. 外部IDを指定します。

e. Amazon Security LakeのIAMロールARN（Amazon Security Lakeのカスタムソース作成の一部として作成されるIAMロール）を指定します。

f. Amazon Security LakeのS3バケットの場所を指定します（これは、Amazon Security Lakeのカスタムソース作成の一部として作成されるS3バケットのことです）。

図3：
セキュリティカスタム
ソースのリソース



g. 「Next」をクリックします。

h. 設定を確認し、「Create Stack」をクリックします。

02

AWS CloudFormation出力のレビュー：

1. この操作の一環としてAmazon SQSキューをデプロイした場合：

   a. スタック作成後、Amazon SQS ARNの「outputs」タブを確認します。

イベント転送のためのSysdig設定

01

IAMユーザーのセットアップ：

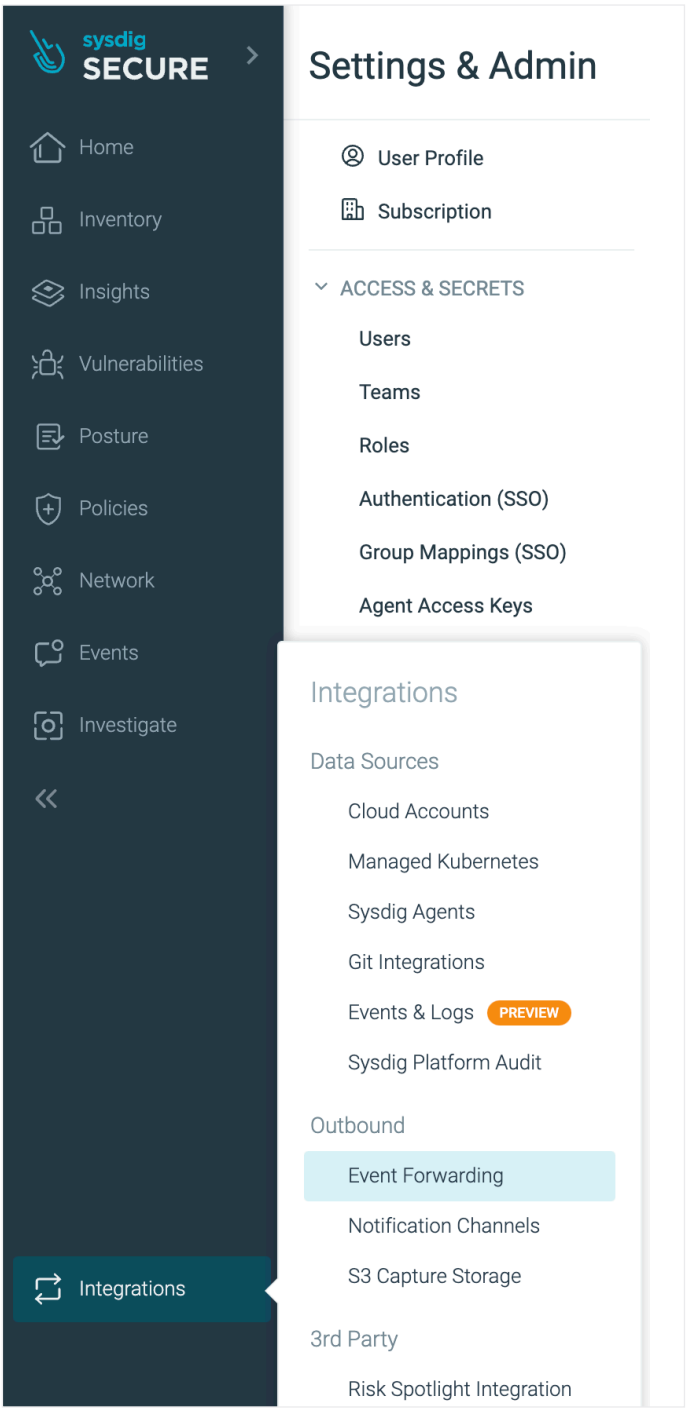
1. Sysdig専用のIAMユーザーを作成するか、既存のユーザーを指定します。
2. サードパーティのサービスを利用するためのアクセスキーを生成します。
3. Amazon SQSにアクセスできるようにアクセスポリシーを調整します。

02

Amazon SQSとの統合：

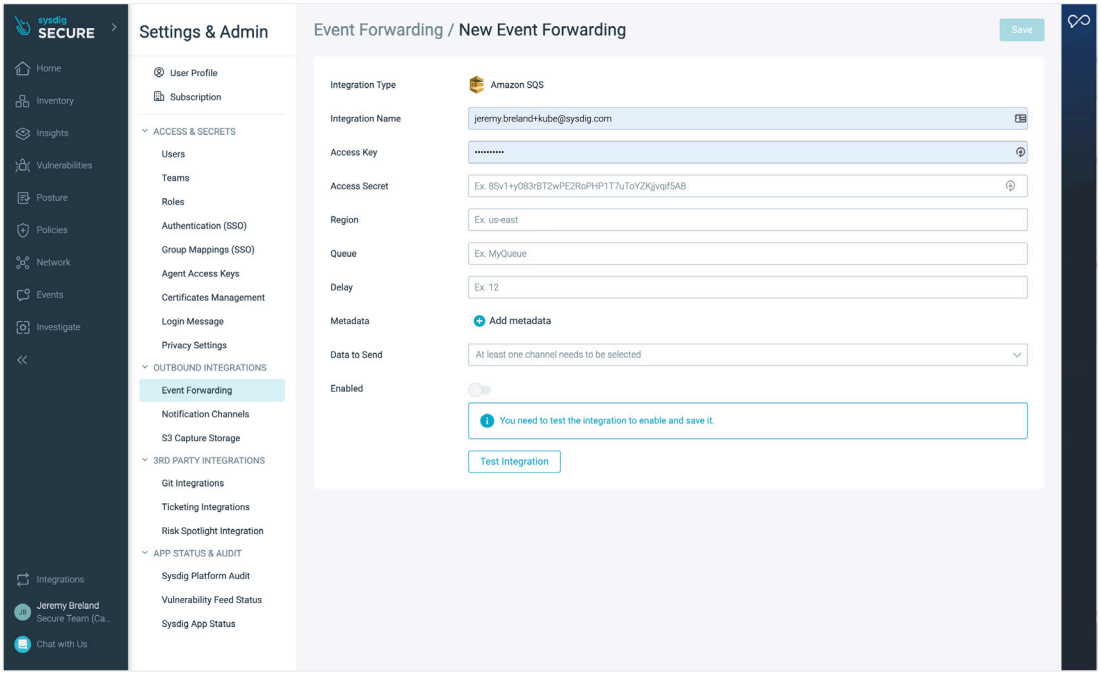
1. Sysdig Secureを管理者権限で使用します。
2. 「Settings」→「Events Forwarding」へと移動します。

図4：
Sysdigのイベント転送
機能へのアクセス



3. 新しい統合を追加し、Amazon SQSを選択します。

図5：
新しいイベント
転送統合の作成



4. Amazon Security Lakeに送信したいデータを選択します。
5. 「Test integration」ボタンをクリックします。
6. 統合をセットアップした後、保存します。

AWS Lambda関数の操作

Amazon SQSイベントのアクティベーション：
AWS LambdaはAmazon SQSメッセージに対して自動的に応答します。

イベントのトランスフォーメーション：

- AWS Lambdaは受信イベントをデコードします。
- デコードされたイベントを、OCSF向けに調整します。

Parquetフォーマットへの変換
効率的な保存を実現するために、OCSF イベントを Parquetへと変換します。

Amazon S3へのデータ転送
Parquetファイルは、指定したAmazon Security Lake S3バケットに保存されます。

テストと検証

Sysdigイベントの生成
イベントをシミュレートするか、リアルタイムのイベントを待機します。

イベントハンドリング
AWS Lambdaは自律的にイベントを解釈した上で、保存する必要があります。

Amazon S3の検証
この時点で、Amazon S3バケットには、イベントの詳細を含むParquetファイルが格納されているはずです。Parquetオブジェクトのパーティショニングスキームは、次の形式に従う必要があります：*<custom source S3 location>/region=<region>/accountId=<accountId>/eventDay=<yyyyMMdd>/parquet files*

監視とデバッグ

AWS Lambdaの監視
AWS Consoleの「Monitoring」タブ内にある「AWS Lambda」セクションにアクセスします。

Amazon CloudWatchとの統合
AWS Lambdaはあらゆるエラーをログに記録します。それらは、トラブルシューティングを容易にするために、対応するAWS Lambda CloudWatchのログに表示されます。

結論

クラウドの動的な環境では、セキュリティデータ分析のための堅牢なソリューションを持つことが、ワークロード、アプリケーション、データの保護を向上させる鍵となります。SysdigとAmazon Security Lakeは、クラウド資産の保護に必要な最新の基盤を提供します。Sysdigの強力なランタイムセキュリティ機能と、スケーラブルでコスト効率に優れたデータレイクを組み合わせることで、組織全体のセキュリティデータをより完全に把握した上で、より効果的なリスク管理を実現できるようになります。

サポート

この統合のソースコードはこちらで閲覧可能です：

ソースコードを見る →

その他のご質問やご意見がございましたら、Sysdigサポートまでご連絡ください。

SYSDIGサポートに連絡する →

GUIDE-020-JA REV.A 3/24