sysdig

AWSクラウドと
コンテナにおける
継続的なセキュリティ

本文の内容は、ホワイトペーパー「Continuous Security for AWS Cloud and Containers」を元に日本語に翻訳・再構成した内容となっております。

AWSクラウドとコンテナにおける継続的なセキュリティ

スピード、アジリティ、スケーラビリティは、もはやITリーダーにとって「あればいい」というものではありません。CIOにとっては、迅速な行動と革新を可能にする最新の基盤を確保することが極めて重要です。

このような要求に応えるためには、これらのニーズをサポートするダイナミックな環境を提供するパブリッククラウドが必要です。また、コンテナアプリケーションの開発やDevOpsのアプローチにより、開発チームがソフトウェアを迅速に立ち上げ、調整を行い、顧客や市場のニーズを満たすソリューションを継続的に提供することが可能になります。

このような変化は、単にデジタル形式のビジネス手法だけではありません。クラウドやコンテナの基本的な部分が、まったく新しいビジネスのやり方を可能にしているのです。これらすべてを実現するために、企業は、クラウドとコンテナのスピードと俊敏性に対応しつつ、より速い結果をもたらすまさにそのプロセスを遅らせることのない、補完的なセキュリティを必要としています。

デリバリーの高速化とセキュリティの確保という2つの目標を同時に達成するためには、データとワークロードを保護しつつ、アジャイルなアプリケーション開発を促進するアプローチが必要です。言い換えれば、「安全でありながら、スピードを落とさない」ということです。

コンテナ、マイクロサービス、ハイブリッドクラウドワークロードなどの新しいパラダイムは、企業がセキュリティを実装する方法を根本から覆しています。コンテナは移植性と分離性に優れているため、アプリケーションを開発環境から本番環境に移行するのに適しています。企業は、初期のサンドボックスから本番環境に移行する際に、クラウドセキュリティとコンプライアンスのプロセスを確立し、コンテナを安全かつ確実に運用するという課題に直面します。クラウドにワークロードをデプロイすると、マイクロサービス間の複雑な相互作用が発生します。サーバーレスインスタンスは流動的なアーキテクチャとして機能し、数分から数秒ごとに変化し、常に変化するセキュリティ環境を作り出します。このような新しいソリューションを使用することで、ビジネスを迅速に進めることができますが、その一方で、新たな潜在的脅威も存在します。

クラウドチームは、アプリケーションを大規模かつ迅速に提供するために、Amazon ECS、Amazon EKS、AWS Fargateなど、Amazon Web Services（AWS）のクラウドおよびコンテナサービスを急速に採用しています。コンテナやオーケストレーションを使用したアーキテクチャーのデプロイに伴い、アプリケーションやインフラストラクチャーのセキュリティ、パフォーマンス、健全性を維持するために必要なことも変化しています。

Sysdig Secure DevOps Platformは、コンテナ、Kubernetes、クラウドを自信を持って実行するためのセキュリティを提供します。Sysdigを活用することにより、ビルドの安全性確保、脅威の検出と対応、クラウドの姿勢とコンプライアンスの継続的な検証を行うことができます。さらに、Sysdigのソリューションは、クラウドインフラストラクチャーとサービスの監視とトラブルシューティングにより、パフォーマンスと可用性の最大化を支援します。Sysdigは、ランタイムでの脅威の検知と対応のためのオープンスタンダードであるFalcoとsysdig OSSを含むオープンソーススタック上に構築されたSaaSプラットフォームを提供しています。

セキュリティ、コンプライアンス、モニタリングを統合したSecure Devopsワークフローを構築することで、企業はデプロイメントを加速し、コンテナワークロードを確実に実行することができます。

AWSコンテナサービス上でのコンテナワークロードのデプロイメントを加速させ、自信を持って本番稼動させることができます。

Sysdigを使用することで、AWSコンテナサービス上でコンテナワークロードを確実に運用することができます。これにより、以下のことが可能になります。

- ビルドプロセスでセキュリティポリシーと構成を検証することで、デプロイメントを高速化
- プロセスの検証による導入の迅速化
- クラウドセキュリティの姿勢とコンプライアンスを継続的に評価
- パフォーマンスに影響を与えることなく、ランタイムの脅威を阻止
- インフラ、サービス、アプリケーション全体のパフォーマンスと健全性を監視して問題を防止
- 詳細な記録を用いたインシデント対応の実施

このガイドでは、AWS環境における包括的なクラウドとコンテナのセキュリティを確立するためのフレームワークを紹介します。

AWSのお客様にとって、セキュリティと可視性が最重要課題である理由

AWSのセキュリティには、データ、アプリケーション、クラウド基盤を保護するために重要な3つの要素があります。

セキュリティに対する責任の共有

AWSのようなパブリッククラウドでは、セキュリティは責任を共有するものです。AWSは環境のセキュリティを担当します。AWSは環境のセキュリティを担当し、お客様は環境内で発生するすべてのことに責任を負います。AWSでは、ユーザー認証、Amazon Simple Storage Service (S3)など、すぐに使えるセキュリティ機能を提供しています。ユーザー認証、Amazon Simple Storage Service (S3)のバケット監視、AWS CloudTrailによるロギングやAWS CloudTrailによる監視などのセキュリティ機能を備えています。しかし、ユーザーは以下の点についても考慮する必要があります。

ワークロード全体の設定ミス、既知の脆弱性、動作の異常をどのように特定し、修正するかを考慮する必要があります。クラウドの継続的な変化には、継続的な監視が必要です。その監視は、クラウドとオーケストレーションのすべてのアクティビティで機能し、使用中のクラウドアセットと監査設定を可視化できる必要があります。また、クラウドとコンテナの活動を継続的にスキャンして分析し、健全性とセキュリティリスクを管理する必要もあります。

自動化による高速化と安全な拡張

セキュリティチームとDevOpsチームは、セキュリティ管理が実際に意図したとおりに機能しているか、また開発作業を妨げていないかを検証する必要があります。多くの企業はこのために手作業でチェックを行っていますが、それでは拡張性に欠けます。自動化はこの問題を効果的に解決する唯一の方法であり、企業は、大規模なデプロイメントであっても、期待通りに動作しているかどうかを理解するために、手動プロセスなしでクラウドアクティビティを分析できるツールを必要としています。自動化されたアプローチでは、クラウドのアクティビティを分析して解釈し、AWS環境内の異常な動作についてDevOpsチームやセキュリティチームに警告することができます。これにより、脆弱性

や問題が悪用されたり、開発プロセスが遅延したり、ビジネスアプリケーションに影響を与える前に対処することができます。

開発の最適化とコンテナオーケストレーション

AWSは2つの重要なコンテナサービス、Amazon Elastic Kubernetes Service（EKS）とElastic Container Service（ECS）を提供しています。それぞれが、包括的なコンテナオーケストレーションシステムとして機能します。これらのサービスは、コンテナ化されたワークロードの安全な作成とデプロイメントをサポートする開発、運用、セキュリティのプロセスを最適化し、コンテナアプリケーションのデプロイメントを加速するように設計されています。ECSとEKSとともに、コンテナ用のサーバーレスコンピュートエンジン「AWS Fargate」も使用できます。

このようなオーケストレーションされたアプリケーション環境では、レガシーなセキュリティツールでは、コンテナの内部を見ることが困難です。また、Kubernetesのダイナミックな性質を扱うことができず、クラスター、アベイラビリティゾーン、リージョンをまたいで拡張することもできないため、もはや機能しません。必要なのは、コンテナ、Kubernetes、クラウド用に構築された、DevOpsのワークフローに統合されたコンテナおよびクラウドセキュリティスタックです。

さまざまなAWSユーザーの固有のニーズに対応

お客様の組織のチームや役割によって、可視性やセキュリティ、ワークロードを本番環境に移行するために必要なプロセスなど、懸念事項や見解が異なります。

開発者

AWSは、開発者がインフラの詳細を知らなくても、クラウドサービス、コンテナ化されたアプリケーション、オーケストレーションを利用できるようにします。AWSの継続的インテグレーションおよび継続的デリバリー（CI/CD）パイプラインは、コンテナ化されたアプリケーションの構築、配布、およびデプロイのプロセスを合理化します。ソースコードとベースイメージを組み合わせるためのAWS CodeBuildやAWS CodePipelineなどのAWSフレームワークを使用して、開発者はGitHubなどのリポジトリに変更をプッシュすることができます。AWSコンテナサービスは、ソースコードからコンテナイメージを作成し、Amazon Elastic Container Registry（ECR）のようなレジストリにプッシュします。コンテナイメージに既知の脆弱性がなく、セキュリティのベストプラクティスに従っていることを確認することは、しばしばアプリケーションの完全性を損なう大きな課題であり、リリーススケジュールを遅らせる原因となります。

クラウド/DevOps

クラウド/DevOpsチームは、アプリケーションとインフラストラクチャーの高可用性、サービス品質、健全性、およびパフォーマンスを維持する責任があります。ユーザーは、AWSウェブコンソールを活用してインフラストラクチャーとプラットフォーム機能を管理し、また、プレイブックを利用してアプリケーションのデプロイメントを自動化します。DevOpsチームは、Falco（オープンソースのクラウドネイティブランタイムセキュリティプロジェクト）、Pod Security Policies、ネットワークポリシーなどの機能を使って、プラットフォームにセキュリティを確実に組み込むことが求められます。

セキュリティとコンプライアンス

セキュリティオペレーション、SecOps、DevSecOps、CSIRTの各チームは、クラウドの共有責任モデルを遵守しています。しかし、脅威の防止、リスクの特定、脆弱性の隔離を効果的に行うために、セキュリティチームはAWSのクラウドやコンテナ環境を継続的に監視し、異常な動作やゼロデイ攻撃から保護するとともに、違反が発生した場合にはインシデント対応を行う必要があります。また、コンプライアンスフレームワークや社内要件に基づいてポリシーを設定し、それをAWS環境で稼働するさまざまなリソースに適用します。さらに、セキュリティチームは、新たに導入されるクラウドインフラストラクチャやアプリケーションを特定して監視し、それらが規制や社内のコンプライアンス要件に適合していることを確認しなければなりません。

SysdigによるAWSコンテナサービスのセキュリティと可視性の管理

統合されたセキュリティ、コンプライアンス、監視により、プライベート、ハイブリッド、マルチクラウド環境において、AWSコンテナサービス上で自信を持ってクラウドネイティブなワークロードを構築、実行することができます。これらの重要な機能を自動化してSecure DevOpsワークフローを実現することで、チームはパフォーマンスの最大化、アジリティの向上、アプリケーションやその他のデータリポジトリ間のデータ統合の最適化、セキュリティリスクの管理、クラウドアプリケーションの迅速な出荷が可能になります。

AWSコンテナサービスは、コンテナプラットフォーム全体（ワークロード、アカウント、ユーザー、およびAWS環境内で発生するすべてのインタラクション）のセキュリティと監視をカバーするベースラインを提供します。アプリケーション、クラスター、ロケーション、クラウドプロバイダの数が増えても、SysdigはAWSコンテナサービスを拡張し、以下のような追加のセキュリティと監視機能を提供します。

- ビルドパイプラインの保護
  - CI/CDパイプラインやレジストリ内のスキャンを自動化します。
  - 脆弱性にフラグを立て、所有者を特定することができます。
  - 脆弱性のあるイメージのデプロイをブロック
- ランタイムの脅威の検出と対応
  - 検出のためのオープンスタンダードであるFalcoを使用してすべての脅威を確認し、ゼロデイ脅威を検知します。
  - Kubernetesのネットワークポリシーでラテラルムーブメントを防止。
  - 詳細な記録を用いてインシデント対応を行う。
- クラウドポスチャーとコンプライアンスの継続的な管理
  - ビルド時やランタイム時に設定ミスやコンプライアンス違反を特定します。
  - アカウントとアクセスのセキュリティを個人およびグループレベルで監視します。
  - 詳細なレポートで進捗状況を確認できます。

    - PCI、NIST、SOC2に対応したすぐに使えるポリシーで時間を節約。
- コンテナ、Kubernetes、クラウドサービスの監視
    - パフォーマンスとキャパシティを監視して問題を未然に防ぎます。
    - 粒度の細かいデータを使用してトラブルシューティングを加速します。
    - Prometheusのモニタリングをクラスターやクラウド全体に拡張します。
    - コンテナのアクティビティを監査し、インシデント対応を迅速化します。

Sysdigは、クラウドとコンテナにおけるセキュリティと監視を統合した、唯一の包括的なプラットフォームを提供しています。クラウドワークロードプロテクションプラットフォーム（CWPP）とクラウドセキュリティポスチャー・マネジメント（CSPM）の機能に加え、健全性とパフォーマンスの監視機能を組み込むことで、クラウドワークロード、アカウント、コンテナ、Kubernetesを網羅する単一の情報源をDevOpsとセキュリティチームに提供します。

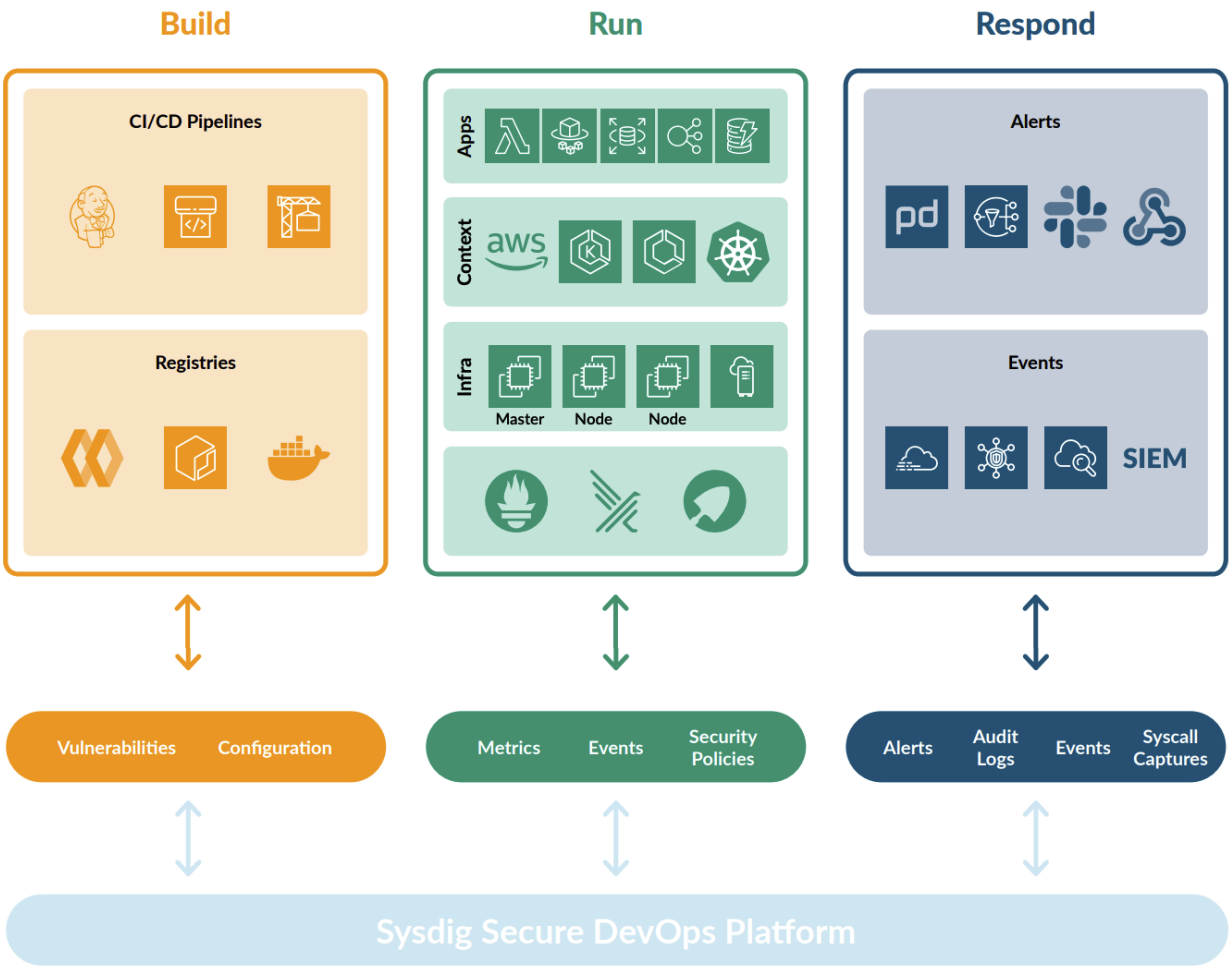
これらのツールは、AWS環境上の統一されたセキュリティと可視性のレイヤーとして動作し、運用、開発、DevOps、セキュリティの各チームに存在する情報のサイロを解消します。Sysdigでは、セキュリティチームとDevOpsチームが、インシデントを正確に特定してトリアージし、原因を迅速に特定して、稼働していないコンテナワークロードに対してもフォレンジックを実行できるようにします。

Sysdigのプラットフォームを利用することで、セキュリティチームやDevOpsチームは、不審なユーザの行動、データへの脅威、特定のネームスペースやクラスターの実行イメージに影響を与える脆弱性など、AWS環境全体のセキュリティ問題を報告することができます。例えば、新しい脆弱性が報告された場合、Sysdigは、DevOpsチームが特定のパブリック・クラウド（AWS）のリージョン、ネームスペース、クラスターなどで影響を受けているイメージや、修正プログラムを所有しているチームを迅速に特定するのに役立ちます。このアプローチでは、クラウドとKubernetesの両方のコンテクストに自動的に相関する脆弱性と粒度の細かいシステムデータを分析することで、問題を迅速に解決することができます。

信頼性の高いセキュアなクラウドアプリケーションの提供を支援し、AWSコンテナサービスを大規模に運用するための集中的な可視性とセキュリティを提供します。Sysdigは、AWSにホストされたSaaSファーストのプラットフォームです。EC2インスタンスごとに1つのエージェントをデプロイすること

で、Sysdigプラットフォームは10,000以上のノードに拡張することができ、AWSコンテナサービスクラスター上で実行されるコンテナやアプリケーションのセキュリティと監視を行います。

ガイド付きオンボーディング、すぐに使えるダッシュボード、厳選されたワークフローにより、すぐに使い始めることができます。Sysdigはクラウド環境と既存のDevOpsワークフローに自動化とすぐに使える統合機能がありますので、可視性とセキュリティ管理に時間がかかることはありません。



Sysdigは、AWSコンテナサービスのコンテナやオーケストレーションに関するインサイトを以下の機能で実現しています。

- ImageVision™ 脆弱性や設定ミスのあるイメージを識別し、デプロイを防止します。

- ContainerVision™ コンテナ内部やマイクロサービス間のリクエストレベルの可視性を提供します。侵襲的な計測を行うことなく、詳細なメトリクスとイベントを提供します。
- ServiceVision™はECSとEKSを統合し、すべてのメトリクスとイベントをオーケストレーションメタデータで自動的に強化します。
- CloudVision™は、クラウドログを使用して、クラウドのアクティビティを統合的に表示します。

AWSコンテナサービスのセキュリティ

ここでは、AWSが提供するさまざまなセキュリティ管理機能と、Sysdigがクラウドネイティブスタックとコンテナのライフサイクル全体にわたってAWSソリューションのセキュリティ、コンプライアンス、監視をどのように拡張するかを見てみましょう。

AWSは以下のようなセキュリティ機能を提供しています：

- Amazon EC2、Amazon Linux 2、Bottlerocketによる安全なホスティングインフラストラクチャー
- AWS Identity and Access Management (IAM)によるアクセスコントロール
- Clair on Amazon ECRによるイメージスキャン
- AWS Configによるコンプライアンスの実施

ホストセキュリティ

クラウドセキュリティは、AWSにとって最優先事項です。お客様は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。マネージドサービスとして、Amazon EC2は、AWSのグローバルネットワークセキュリティ手順によって保護されています。

AWSは、環境へのアクセスを制限することができるEC2インスタンスのホストベースの制御を含む、レイヤードアプローチの使用を推奨しています。通常、企業は、ネットワークトラフィック、ホストレベルのアクセス、および対応するログファイルを監視および分析するホストベースの侵入検知システム（HIDS）を採用します。Amazon CloudWatchは、HIDSからのアラートを収集・配信するための標準的なソリューションです。

AWS上でコンテナを安全に運用するために、AWSはクラウドネイティブアプリケーションを実行するための安全で安定した高性能なOSを提供しています。これには、Amazon Linux 2とBottlerocketが含まれます。

- **Amazon Linux 2**は、デフォルトでセキュアな次世代のAmazon Linuxです。クリティカルでないパッケージの数を減らし、潜在的なセキュリティ脆弱性への暴露を制限します。Amazon Linux 2

では、「クリティカル」または「重要」と評価されたセキュリティアップデートが初回起動時に自動的に適用されます。

- **Bottlerocket**は、仮想マシンやベアメタルホスト上でコンテナを実行するためにAWSが専用に開発した、Linuxベースのオープンソースのオペレーティングシステムです。Bottlerocketには、コンテナの実行に不可欠なソフトウェアのみが含まれているため、リソースの使用率が向上し、セキュリティの攻撃対象を減らし、管理のオーバーヘッドを低減します。Bottlerocketでは、セキュリティアップデートが利用可能になり次第、最小限の中断で自動的に適用することができ、障害が発生した場合にはロールバックすることができます。

これらのソリューションは、クラウド上での安全な運用に加え、AWS Outpostsを利用したオンプレミス施設でも利用することができます。Sysdigは、Amazon Linux 2とBottlerocketの両方で、パブリック、プライベート、およびハイブリッドのデプロイメントにおけるセキュリティ、監視、およびコンプライアンス機能を検証しました。従って、これらのソリューションをAmazon EKSやECSと組み合わせて使用することで、お客様が安全かつ一貫してコンテナワークロードを本番環境で実行できることが保証されます。

認証と認可

AWS Identity and Access Management (IAM)は、管理者がAWSサービスに安全にアクセスし、統合し、対話する仕組みを提供しています。これにより、企業は個人やグループに許可を与えることができます。管理者は、一元化されたソースから、ロール、組織、地域、またはワークロードやその他のリソースのセキュリティ維持に関連するその他のカテゴリに基づいて、アクセスを許可または拒否することができます。

ユーザーは、AWSの認証情報に基づくリクエストにより、さまざまなサービスにアクセスします。ただし、S3ストレージのような一部のリソースについては、粒度の細かいパーミッションを付与することで、そのソースのみに固有のアクセスを提供することができます。リクエストのコンテキストは、AWSのユーザーが自分の環境に適用するポリシーに基づいて評価されます。ポリシーはJSONドキュメントとして保存され、パーミッションの事実上のソースとして機能します。

AWSサービスへの具体的なアクセスは、Web UI、CLI、APIなどの標準的なインターフェースを通じて提供されます。さらに、サービスはAWSコンテナサービスと相互作用するため、オーケストレーションの状態を認識し、これらのプラットフォームに対してアクションを実行することができます。CI/CDパイプラインが新しいデプロイメントを本番環境にプッシュすることを想像してみてください。誰が何をできるかをどのようにコントロールし、測定するのでしょうか？

AWSが提供するのは...

AWS IAMは、AWSのサービスやリソースへのアクセスを安全に管理することができます。IAMを使用すると、AWSユーザーとグループを作成および管理し、パーミッションを使用してAWSリソースへのアクセスを許可または拒否することができます。IAMの管理者は、EKS、ECS、Fargateのリソースを使用するために認証（サインイン）し、許可（パーミッション）できる人を制御します。

Sysdigが追加するのは...

Sysdigでは、AWSコンテナサービスの可視化、メトリクス、通知、セキュリティポリシーのいずれかにアクセスできる人を定義できます。これは、Sysdig Teamsとして知られており、既存のAWS IAMメカニズムを補完するために、サービスとメタデータベースのアクセスコントロールの概念を導入しています。

Sysdig Teamsでは、AWS上にデプロイされた特定のサービスや限定されたサービス群へのアクセス権を持つユーザのグループを定義することができます。例えば、アプリケーションの所有者は、特定のネームスペースにあるイメージの脆弱性スキャン結果のみを見ることができます。アクセスコントロールで公開範囲を制限し、特定のチームごとにデフォルトの設定を提供することで、ユーザやチームのセキュリティ情報を効率化することができます。

Sysdigは、ユーザの権限を定義するロールベースアクセスコントロール（RBAC）をサポートしており、組織内の異なるチーム間で連携したアクセスコントロールを提供しています。管理者ロールに加えて、閲覧のみ、標準ユーザー、上級ユーザー、チームマネージャーなど、さまざまなアクセスロールが用意されています。

イメージスキャン

コンテナアプリケーションやインフラコンポーネントは、すぐに利用できるパッケージの上に構築されています。その多くはオープンソースソフトウェアであり、古いライブラリのバージョンが含まれている可能性があります。これらのパッケージがどこから来たのか、誰が作ったのか、そしてその中に既知の脆弱性があるかどうかを知ることは重要です。

AWSが提供するのは...

Amazon Elastic Container Registry（ECR）は、完全に管理されたDockerコンテナレジストリであり、開発者がDockerコンテナイメージを簡単に保存、管理、デプロイすることができます。Amazon ECRは、ECSやEKSなどのAWSコンテナサービスと統合されており、開発から本番までのワークフローを簡素化します。

ユーザーがAWS上でコンテナを採用し始めると、ECRスキャンは継続的なセキュリティとコンプライアンスを提供するための最初のステップとなります。ECRは、オープンソースのClairプロジェクトが提供するCVE（Common Vulnerabilities and Exposures）データベースを使用して、スキャン結果のリストを提供します。AWS上で動作するアプリケーションが悪用されないように、ECRから取得したイメージを脆弱性と設定ミスの両方について確実にスキャンする必要があります。

Sysdigが追加するのは...

Sysdig Secureは、Kubernetesのライフサイクルのすべての段階でセキュリティとコンプライアンスを実現します。15以上のCVE脅威フィードを活用し、Sysdig Secureは脆弱性やセキュリティ、コンプライアンス関連の設定ミスを検出する単一のワークフローを提供します。チームがアプリケーションを構築する際、Sysdigは脆弱なイメージがCI/CDパイプラインでプッシュされるのを防ぎ、本番環境で新たな脆弱性を特定します。

Sysdig Secureは、ECRのデフォルトのイメージ・スキャンに加えて、ECRのスキャン機能を提供します。ECRと一緒に設定すると、Sysdig Secureはレジストリに保存されているイメージを分析のためにエンジンに取り込みます。これにより、デプロイ前に脆弱性、コンプライアンスチェック、設定ミスなどをスキャンすることができます。脆弱性は、ベースイメージ、OSパッケージ、PIPのPythonパッ

ケージなどのサードパーティライブラリ、開発者が本番前にアプリケーションイメージに取り込んでいる可能性のあるJava JARファイルなどから検出できます。

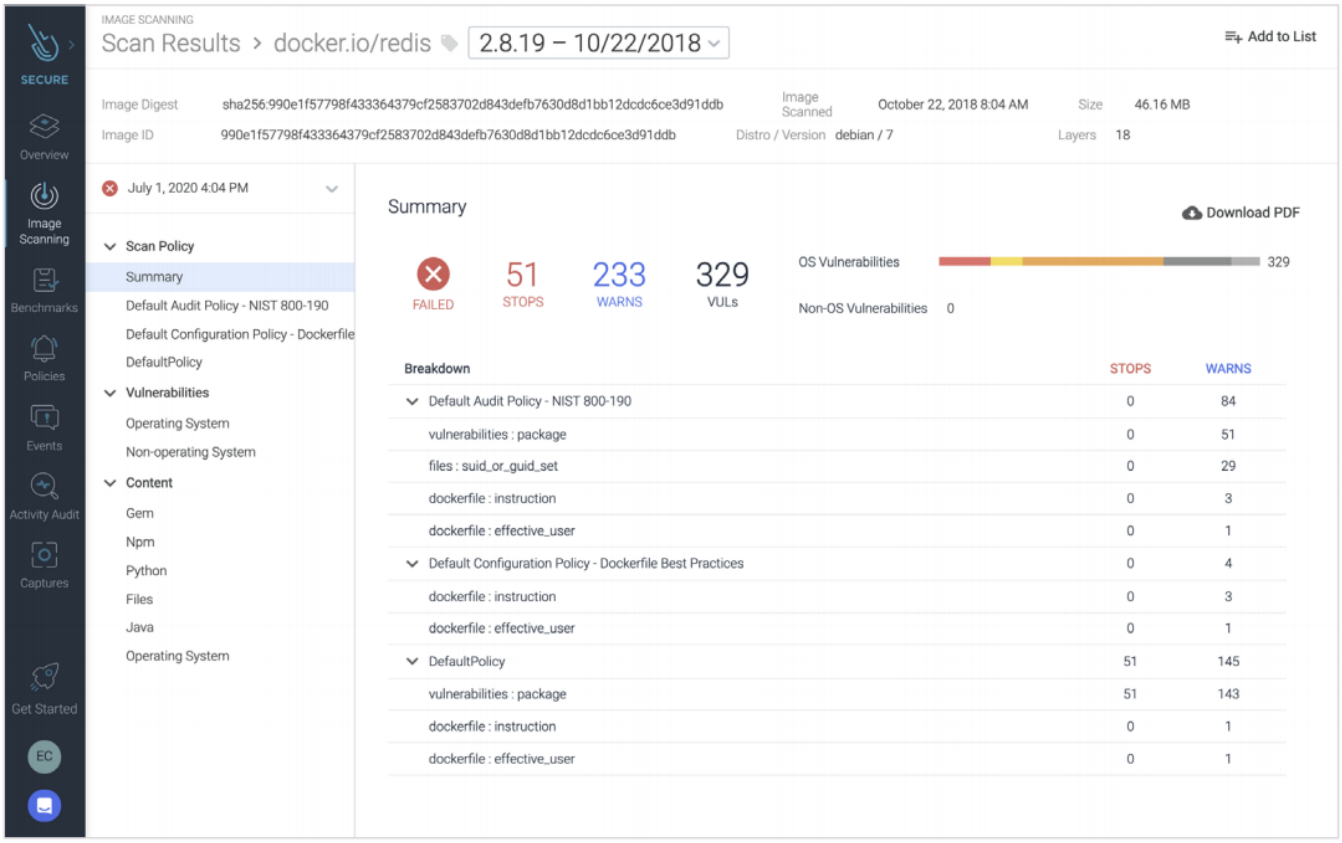
デプロイメント前のスキャンに関しては、Sysdigは2つのコンテナイメージスキャンオプションを提供しています。

- 標準的な方法では、イメージをSysdigに送ってスキャンしてもらいます。スキャン後、Sysdig Secure UIでスキャン結果を確認することができます。
- インラインスキャンとも呼ばれるローカルスキャンは、CI/CDパイプラインやECRレジストリ内で直接イメージをスキャンします。このオプションでは、レジストリの認証情報やイメージのコンテンツをAWS環境の外で共有する必要がないため、より安全なアプローチが可能です。また、スキャンを自動化し、ECR内で直接レポートを生成することで、スキャン結果を迅速に得ることができます。

Sysdig Secureは、以下を可視化します：

- OS公式パッケージの脆弱性
- 非公式なパッケージの脆弱性
- 設定のチェック（例：DockerfileでSSHを公開している、ユーザがrootで実行しているなど）
- JavascriptのNPMモジュール、PythonのPiP、RubyのGEM、JavaのJARアーカイブなどのサードパーティ製ライブラリの脆弱性
- GEM、Java JARアーカイブなどのサードパーティライブラリの脆弱性
- シークレット、トークンや証明書などの認証情報、およびその他の機密データ
- 既知の脆弱性と利用可能な更新プログラム
- メタデータ（イメージのサイズなど）
- NIST 800-190、PCIなどのフレームワークのコンプライアンスチェック

これらの成果物は保存され、特定のレジストリ、リポジトリ、またはイメージタグに指定できるカスタムスキャンポリシーに照らして評価されます。Sysdig Secureのスキャンポリシーは、イメージ内の脆弱性、設定ミス、コンプライアンス上の問題を検出し、UIで直接合否結果を生成します。



Fargateイメージのローカルスキャン

Fargateユーザーにとって、Sysdigのソリューションならではの特徴は、Fargateタスクの開始時にECR内のイメージのスキャンをトリガーする機能です。Amazon EventBridgeを利用して、SysdigはFargateのリクエストを傍受し、イメージを識別してスキャンを実行します。この自動化されたローカルスキャン機能は、サーバーレスプラットフォーム上で実行することを意図したコンテナのセキュリティを確保するのに役立ちます。

CI/CDパイプラインのセキュリティ

CI/CDパイプラインは、ビルドやテストなどのソフトウェアデリバリープロセスのステップを自動化し、チームが顧客にアップデートをより早く、より頻繁に提供できるようにします。アプリケーションを構築する際に、デリバリパイプラインにセキュリティを組み込むことで、脆弱性の特定と対処を迅速に行い、開発者の生産性を維持することができます。

AWSが提供するのは...

AWSでは、ソフトウェアデリバリープロセスを自動化するために、継続的インテグレーション／継続的デリバリーパイプラインを設定することができます。いくつかのツールは、DevOpsチームがソフトウェアデリバリープロセスを自動化するのに役立ちます。バージョン管理のためのCodeCommit、コードの構築とテストのためのCodeBuild、コードの自動デプロイのためのCodeDeployです。これらのツールに加えて、CodePipelineはこれらの異なるステージを可視化し、自動化することができます。

AWS CodeBuildは、ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを生成する、フルマネージドの継続的インテグレーションサービスです。CodeBuildは、継続的にスケールアップし、複数のビルドを同時に処理するため、ビルドがキューの中で待たされることはありません。

AWS CodePipelineは、アプリケーションやインフラストラクチャーの更新のためのリリースパイプラインを自動化する、フルマネージドの継続的デリバリーサービスです。CodePipelineは、定義されたリリース・モデルに基づいて、コードが変更されるたびに、リリース・プロセスのビルド、テスト、デプロイの各フェーズを自動化します。

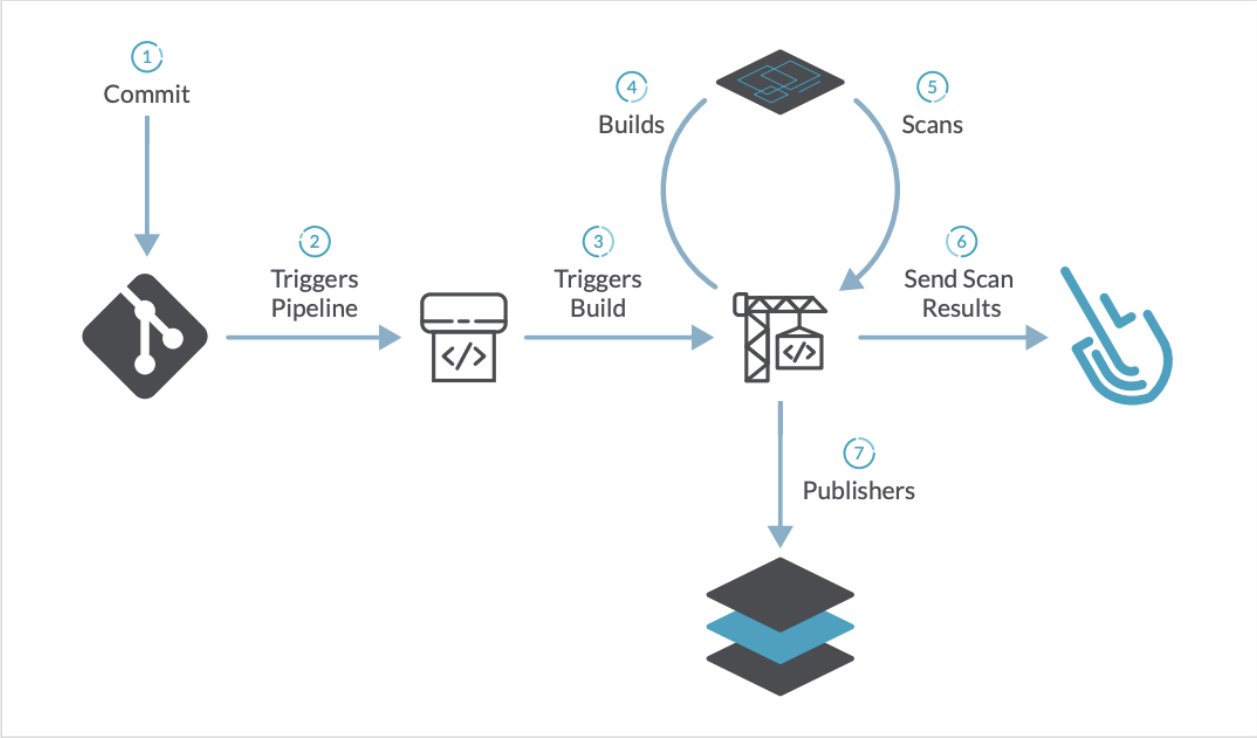
Sysdigが追加するのは...

AWSで使用されるCI/CDパイプライン用のイメージスキャンは、パイプラインの初期段階で既知の脆弱性を検出し、コンテナのビルド構成を検証することで、デプロイメントのセキュリティに対するDevOpsチームの信頼性を高めます。イメージがコンテナレジストリに公開されたり、本番環境にデプロイされたりする前にこれらの問題を検出することで、修正を迅速に適用し、本番環境へのデリバリー時間を改善することができます。

Sysdig Secure Image Scanningは、AWS CodeBuild、AWS CodePipeline、Jenkins、Bamboo、GitLab、CircleCI、Tektonなど、お使いのCI/CDパイプラインに直接統合できます。サードパーティのライブラリ、公式/非公式のOSやパッケージ、設定チェック、クレデンシャルの公開、メタデータなどの脆弱性や設定ミスをキャッチすることができます。Sysdigのローカルインラインスキャンを使えば、イメージがレジストリにプッシュされる前に問題を検出できます。

CI/CDパイプラインに統合されたSysdigのスキャンは、開発者が必要とする情報をCI/CDツール内で直接提供し、スキャンが失敗した理由と修正すべき点を理解することができます。クリティカルではないポリシー違反に対しては、パイプラインを中断することなく、コンテナイメージのセキュリティを向上させるために何を変更すべきかを警告します。

Sysdigを使用することで、AWS CodePipelineを使用して構築されたイメージは、イメージをインフラストラクチャーから外すことなく、またステージングレジストリを使用することなくスキャンすることができます。また、複数のスキャンを並行して実行できるため、スループットが向上します。



イメージアシュアランス

イメージアシュアランスは、承認されていないイメージがコンテナ環境にデプロイされるのを防ぐことに重点を置いています。本番環境で実行する前に、定義されたポリシーに基づいてイメージを評価・検証することで、問題やエラーを減らすことができます。

AWSが提供するのは...

KubernetesのアドミッションコントローラをEKSと併用することで、オーケストレーションされたコンテナクラスターに承認されていないイメージがデプロイされるのを防ぐことができます。このKubernetesの機能を使って、EKSはKubernetes APIへのリクエストの評価をサポートし、定義されたセキュリティ要件を満たさないリクエストを拒否します。

Sysdigが追加するのは...

EKSはSysdig Secureをチェックして、イメージが設定されたセキュリティポリシーに準拠しているかどうかを評価することができます。アドミッションコントローラを使用している場合、このセキュリティ検証の判断はAPIに伝搬され、APIは元の要求者に返信し、イメージがチェックに合格した場合のみオブジェクトをetcdデータベースに持続させます。

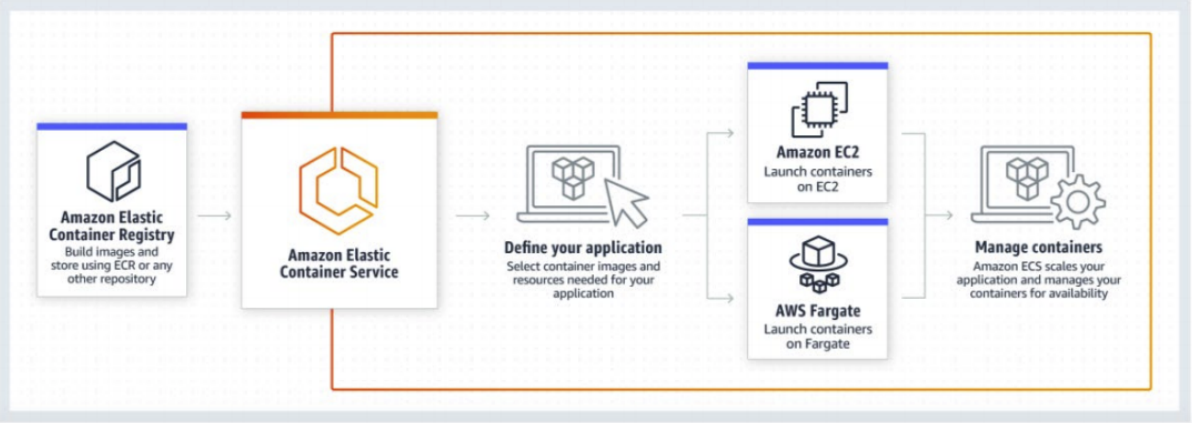
レジストリセキュリティ

コンテナイメージのセキュリティに加えて、レジストリ自体のセキュリティも、組織のリスクを低減するための重要なステップです。RBAC を使用してコンテナイメージをプル／プッシュできる人を管理したり、プライベートレジストリを使用したりすることは、組織を保護するための手段のひとつです。

AWSが提供するのは...

Amazon ECRは、セキュアでスケーラブル、かつ信頼性の高いマネージドAWS Dockerレジストリサービスです。Amazon ECRは、AWS IAMを使用したリソースベースのパーミッションを持つプライベー

トDockerリポジトリをサポートしており、特定のユーザーやAmazon EC2インスタンスがリポジトリやイメージにアクセスできます。開発者は、Docker CLIを使用してイメージをプッシュ、プル、管理することができます。



Sysdigが追加するのは...

Sysdig Secureのコンテナイメージスキャンは、CoreOS Quay、Amazon ECR、DockerHub Private Registries、Google Container Registry、Google Cloud Artifact Registry、JFrog Artifactory、Microsoft ACR、SuSE Portus、VMware Harborなど、Docker v2互換のレジストリをすべてサポートしています。

コンプライアンス

AWS上でマイクロサービスを実行する企業のコンピューティング環境は、何百、何千もの相互接続されたアプリケーションやサービス、そして大規模で多様なユーザーで構成されています。この広大な環境のセキュリティを管理するためには、システムがセキュリティポリシーに準拠しているかどうかをスキャンする標準的な方法が必要です。

AWSが提供するのは...

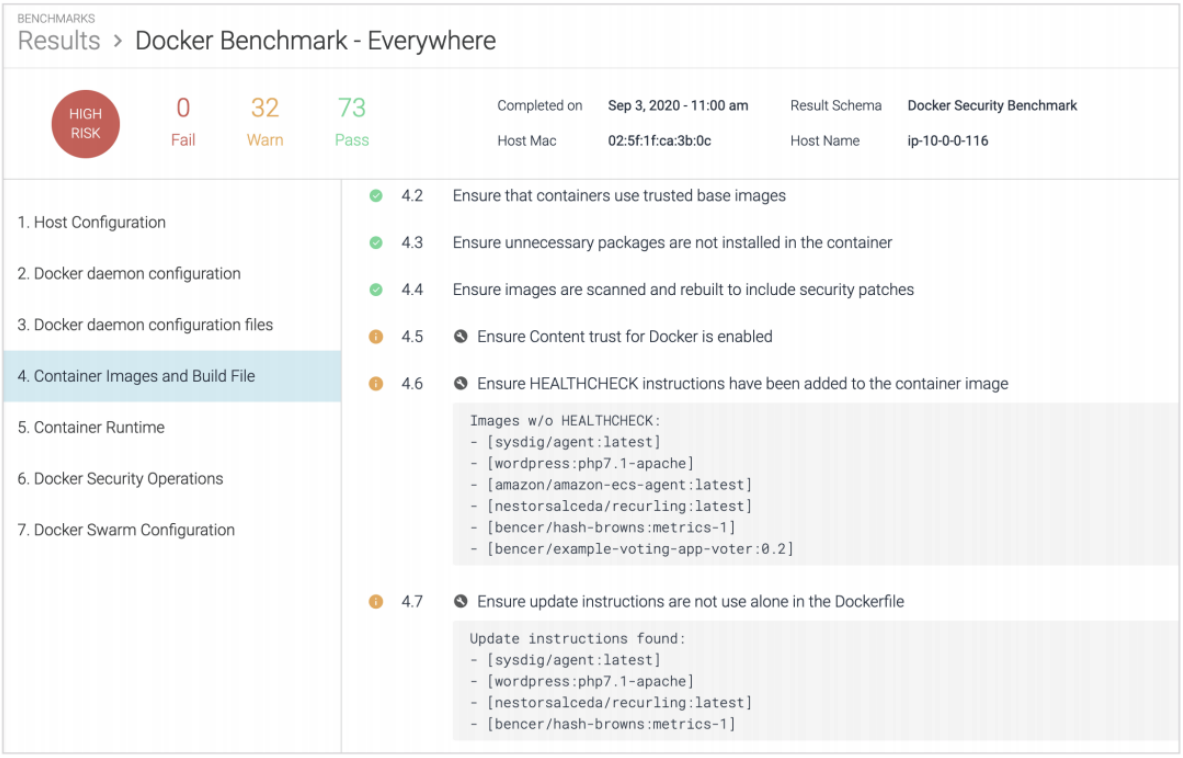
AWS Configは、お客様のAWSリソースの構成を評価、監査、査定することができるサービスです。AWS Configは、AWSリソースのサービス構成を継続的に監視・記録し、記録された構成と望ましい構成との評価を自動化することができます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、および運用上のトラブルシューティングを簡素化することができます。

Sysdigが追加するのは...

Sysdigは、NISTやPCIなどの規格に対応したコンテナのライフサイクル全体のコンプライアンスを拡張します。デプロイメントが望ましい設定に準拠しているかどうかを検証できることは、コンプライアンスの最初のステップの1つです。しかし、コンプライアンス要件はそれだけではありません。コンテナのコンプライアンスには独自の要件があり、様々なポイントで実施する必要があります：

- AWS、Docker、Kubernetes向けのCenter for Internet Security（CIS）ベンチマークを使用して、クラウド、コンテナ、インフラストラクチャーのセキュリティのベストプラクティスをチェック。
- ビルド時には、コンテナイメージのスキャンポリシーをNIST 800-190、PCI、HIPAAなどの標準にマッピング。
- ランタイム時には、MITRE ATT&CKのような攻撃フレームワークを継続的に検出するためのポリシーを使用したり、デプロイ後にコンプライアンスをチェックしたりします。
- SOC2、PCI、ISO、HIPAAの要件の一部である、コンテナ環境のあらゆる変更を監査する。

Sysdigでは、コンプライアンスダッシュボードを使って進捗状況を確認することができます。Sysdigは、インフラストラクチャーレイヤーを始めとして、ホスト、プラットフォーム、コンテナのコンプライアンスチェックを行います。例えば、AWS Foundationベンチマーク、Kubernetesベンチマーク、Docker CISベンチマークなどがあります。また、ポリシー違反を修正するためのレメディエーションガイダンスも提供します。これにより、設定上の問題が発生した際に、より迅速に解決することができます。



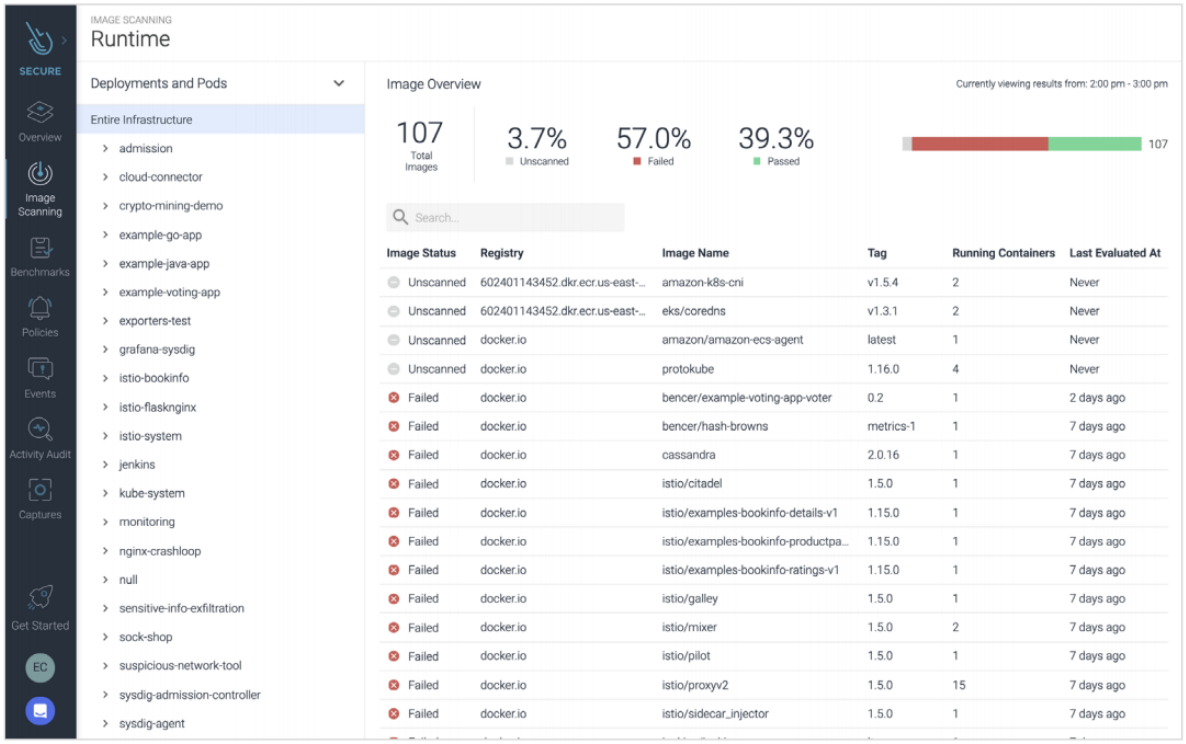
Sysdig Secureは、コンテナイメージのセキュリティと、NIST SP 800-190、PCI DSS、Dockerfileなどのコンプライアンスのベストプラクティスを実施するためのツールを提供します。Sysdig Secureのコンテナイメージスキャンポリシーを使用することで、クラウドのコンプライアンスを検証し、以下のようなベストプラクティスをイメージレベルで実施することができます。

- イメージ・サイズの制限
- GPlv2ライセンスのブラックリスト化
- コンテナが信頼できるベースイメージと必要なパッケージのみを使用するようにする。

Sysdigは、NIST SP 800-190、PCI DSS、CISベンチマーク、HIPAA、GDPR、MITRE ATT&CKフレームワークなどの主要なセキュリティ標準を最新のセキュリティポリシーセットに変換することで、ランタイムコンプライアンスを保証します。Sysdigは、デプロイ後のコンテナの動作を分析し、ランタイムドリフティングを監査します。Sysdigは、システム上で実行されたあらゆるコマンド（ホストと

コンテナ内の両方、docker execやoc attachなど）やKubernetes APIを監査目的で利用します（シークレットリソースへのアクセス、許可されていないユーザによるリクエストなどの監査）。

新規に高/クリティカルなCVEが公開されると、すぐにエクスポージャーを評価することができます。影響を受けたサービスや説明責任のあるチームを迅速に特定できます。開発者やアプリケーションの所有者は、サービス、デプロイメント、アプリケーションなどのKubernetesやクラウドのメタデータを使って特定され、イメージや脆弱性を閲覧するようアラートが出されます。



ネットワークセキュリティ

アプリケーションがコンテナやクラウドに移行することは、セキュリティモデルを見直すきっかけになります。クラウドチームの多くは、組織内のネットワークであっても認証と許可を必要とするゼロトラストのアプローチをとっています。

ネットワークをセグメント化し、分離し、制御する能力は、ゼロトラストのための重要な制御ポイントであり、コンテナやKubernetes環境でより効果的なセキュリティを実現するために、ますます不可欠になっています。

適切なツールがなければ、DevOpsチームはコンテナ化されたアプリケーションがどのように通信しているかを確認することができず、オープンネットワークポリシーを利用した悪意のある試みを見逃してしまう可能性があります。アプリケーションがどのように使用されているかを知ることなく、Kubernetesでゼロトラストのネットワークセキュリティモデルを適用することは困難です。

AWSが提供するのは...

AWS上のコンテナ化されたアプリケーションは、通常、クラスター内で実行されている他のサービスや、外部のAWSクラウドサービスへのアクセスを必要とします。AWSは、特定のEC2セキュリティグループをEKSクラスターで稼働するポッドに直接割り当てることで、Kubernetesのネットワークセキュリティに対応しています。

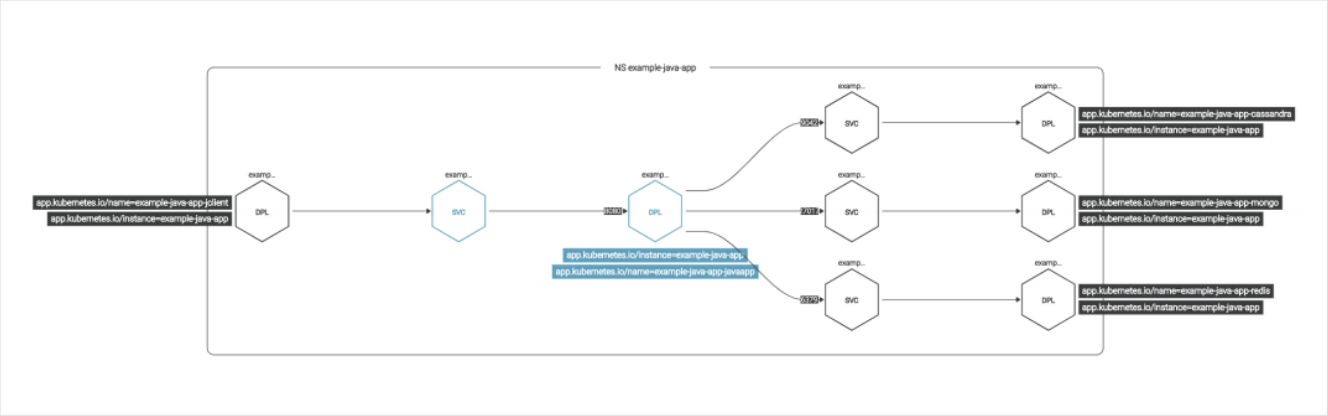
ポッドのセキュリティグループは、さまざまなネットワークセキュリティ要件を持つアプリケーションを共有コンピュートリソース上で実行することで、ネットワークセキュリティのコンプライアンスを実現します。

ネットワークセキュリティルールをEC2セキュリティグループ内で定義し、KubernetesネイティブAPIを持つアプリケーションのポッド間およびポッドから外部のAWSサービスへのトラフィックに適用できます。このアプローチでは、AWSセキュリティグループポリシーで運用知識とツールを再利用して、ネットワークと認証のレイヤーでセキュリティを実装することができます。

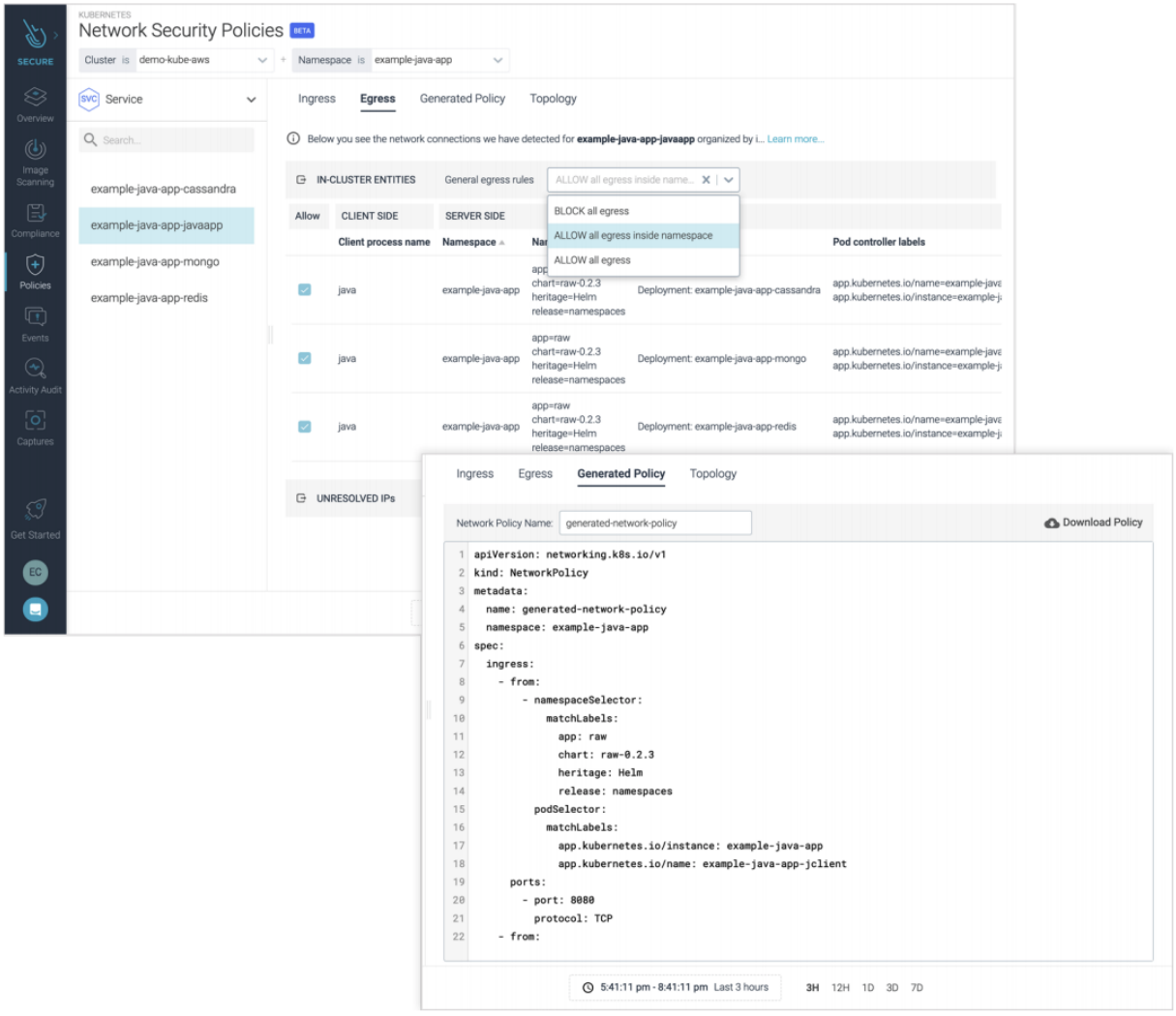
Sysdigが追加するのは...

Kubernetesのネットワークポリシーは、クラスター内のネットワークトラフィックを制御し、ネットワークセキュリティを実現するためのネイティブなオプションを提供します。Kubernetesネイティブな制御により、Kubernetesがネットワークのマイクロセグメンテーションを実施するため、パフォーマンス、信頼性、セキュリティが向上します。しかし、Kubernetesのネットワークポリシーは、適切なアプリケーションの知識とKubernetesの専門知識がないと実装するのが難しいという課題があります。Sysdigはこれらの障壁を取り除き、Kubernetesコントロールによるゼロトラストネットワークセキュリティの実装を簡素化します。

Sysdig Secureは、システムコールを可視化することで、EKSポッド、サービス、アプリケーションのすべてのネットワークトラフィックを自動的に検出します。データはKubernetesのコンテキストとラベルで自動タグ付けされ、Kubernetesネットワークポリシーの実装を簡素化するために使用されます。



ダイナミックトポロジーマップでは、アプリケーションやサービス間のすべてのネットワーク通信を可視化し、特定の時間枠でのトラフィックフローを掘り下げて確認することができます。この情報をシンプルなUIで利用することで、セグメンテーションを適用し、接続を許可またはブロックするネットワークポリシーを精緻化することができます。Sysdigは、ポリシーをKubernetesクラスターに適用するために使用できるYAMLファイルを自動的に生成します。



さらに、Sysdig Secureはすべての接続と接続を確立しているプロセスのフィンガープリントを取ることができます。この監査タップ機能により、クラウド担当者は、ラベルを含むコンテキストを完全に可視化した上で、ネットワークアクティビティをきめ細かなレベルで調査することができます。NISTやPCIなどの規制を受けている企業は、この機能をネットワークセグメンテーションとともに活用し、コンプライアンス要件を満たすことができます。

Sysdigは、コミュニティによって吟味されたオープンな標準ベースのアプローチに基づいてゼロトラストネットワークセキュリティを実現し、Kubernetesがエンフォースメントを提供することで、パフォーマンス、信頼性、セキュリティを向上させます。これにより、マンインザミドルのエンフォー

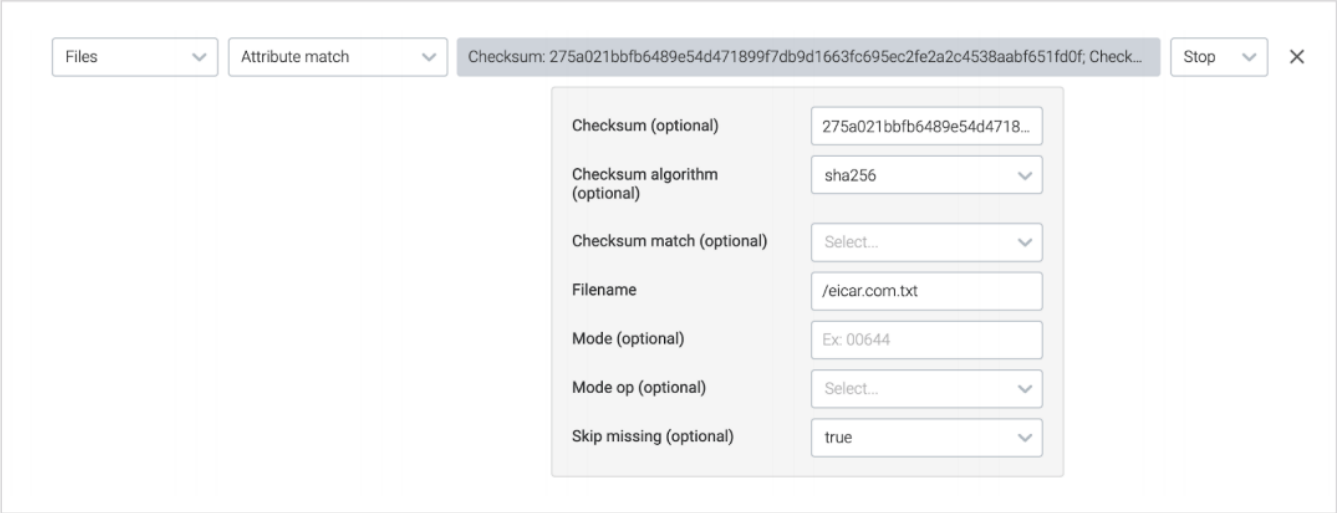
スメントメカニズムが不要になります。使いやすいインターフェースを提供し、Kubernetesの専門知識を持たないチームのためにガードレールを自動化することで、SysdigはAWSユーザーの時間を節約し、ネットワークセキュリティのリスクを低減します。

ファイル整合性監視（FIM)

ファイル整合性モニタリングは、機密性の高いファイル関連のアクティビティをすべて可視化します。重要なシステムファイルやディレクトリの改ざん、不正な変更などを、悪意のある攻撃であるか、計画外の運用活動であるかに関わらず検出します。

Sysdig Secureでは、特定のファイル属性をスキャンして、CI/CDパイプライン内のイメージスキャンポリシーの一部として埋め込むことができます。これにより、FIMポリシーが満たされていない場合、ビルドを早期に失敗させることができます。ファイル整合性監視ポリシーでは、以下のことが可能です。

- ファイルが存在するかどうか、あるいは見つからないかどうかをチェックし、条件に応じてアラートを発生させる。
- 特定のファイルをそのSHA256ハッシュと照合して検証する。コンテナ内のバイナリに変更が加えられた場合、疑わしい、潜在的に危険なものとしてフラグが立てられます。
- ファイルのパーミッションを検証します。例えば、ファイルに予期しないところで実行可能ビットがある場合に警告することができます。
- 正規表現に基づいてファイル名をチェックします。
- コンテンツを検査し、露出したパスワードやクレデンシャルのリークを探します。



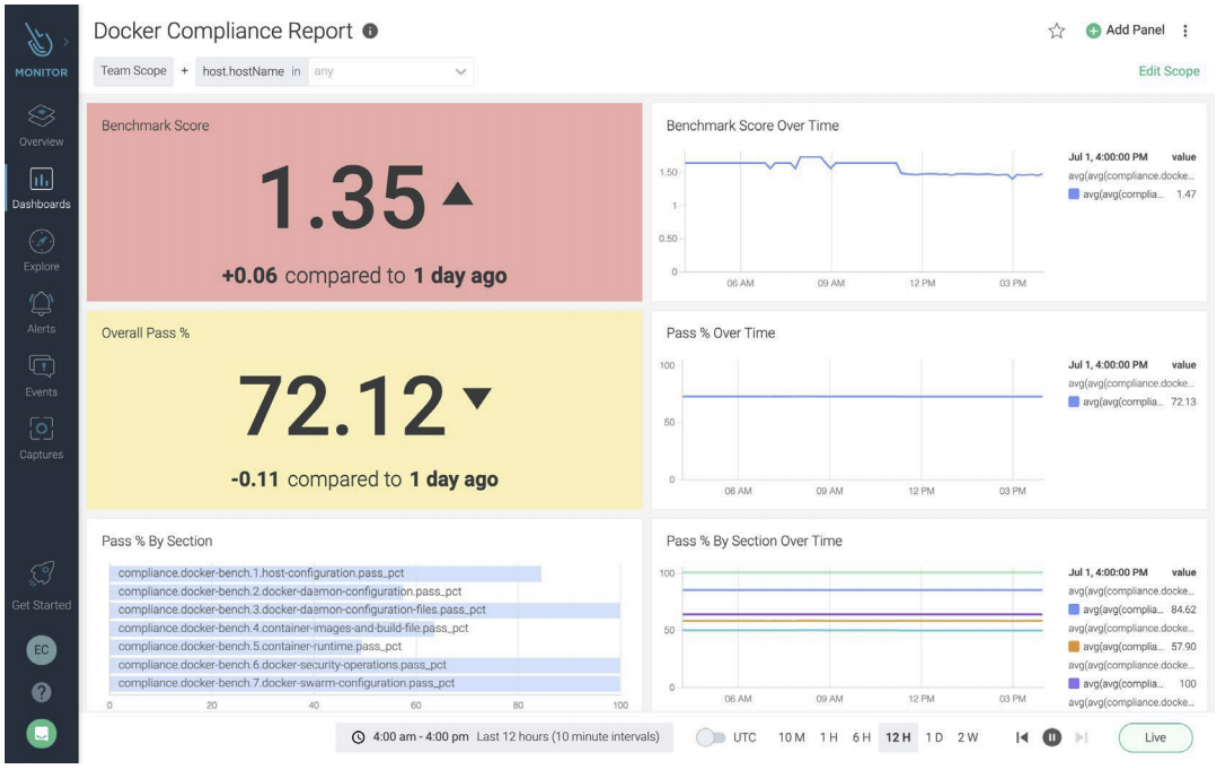
また、ランタイムにFIMポリシーを実装して、ファイルシステムへの疑わしい変更を警告することもできます。これらは、強力なセキュリティ態勢を強化するためにルールとして含めるべき、一般的なファイル整合性監視チェックです。

- ファイルまたはディレクトリの作成または削除
- ファイルやディレクトリの名前の変更
- パーミッション、オーナーシップ、継承など、ファイルやディレクトリのセキュリティ設定の変更
- コンテナのファイルの変更
- コンテナのパス以下のファイルの変更
- bash履歴の削除

Sysdigのプラットフォームは、堅牢なレポートを作成するだけでなく、セキュリティベンチマークを一連のセキュリティメトリクスやダッシュボードに変換します。内部および外部のコンプライアンスおよび監査チームは、自社のセキュリティ状況を分析し、パターンやトレンドを迅速に視覚化して、コンプライアンス体制に関する貴重な洞察を得ることができます。

- 自社のセキュリティ状況を過去の任意の時点と比較する
- アプリケーションおよび環境全体のリスクおよびコンプライアンスの状況を把握する
- コンプライアンスチェックが受け入れられたポリシーを下回った場合に警告する

- AWSコンテナクラスター間のコンフィギュレーションドリフトの検出



ランタイムセキュリティ

セキュリティ監視

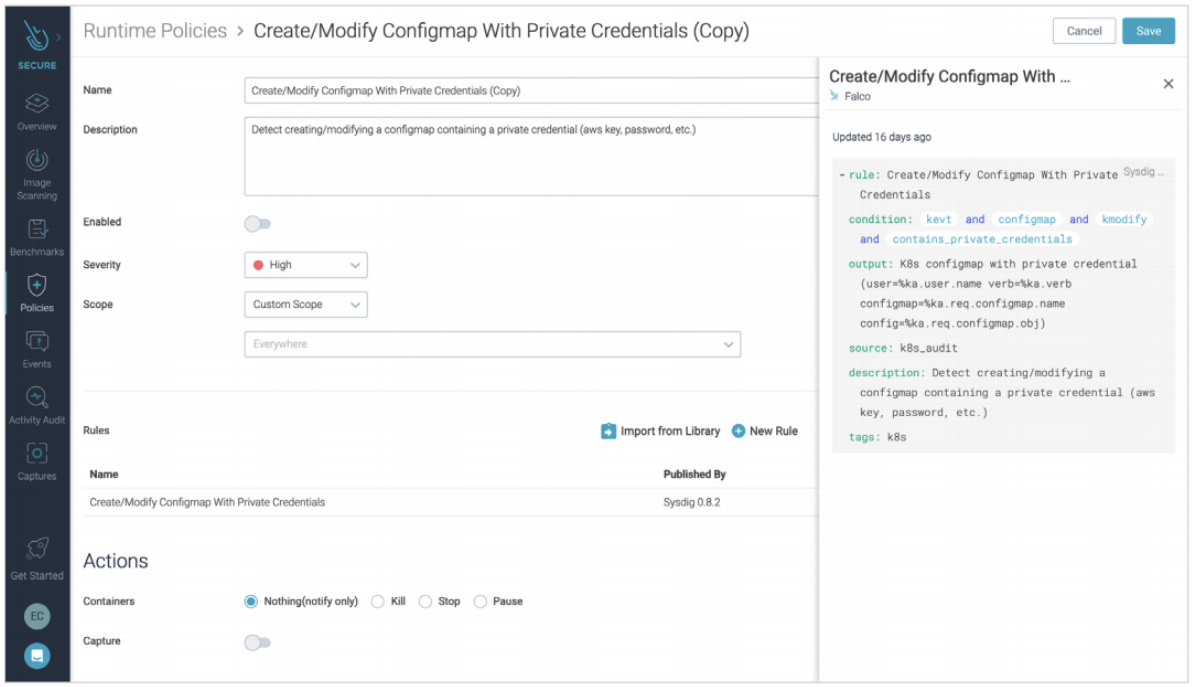
AWSコンテナサービスの監視とセキュリティの両方を可視化することは、変革の旅を成功させるために必要です。例えば、セキュリティチームは、クリプトマイニングやサービス拒否（DoS）攻撃が、特定のパフォーマンスメトリクスの異常な逸脱によってさらに説明できるかどうかを知る必要があります。

さらに、本番環境に入ってからは、最低限の権限とアクセス許可でアプリケーションを構成し、リスクを低減することが重要です。同時に、ワークロードの挙動を観察し、異常なアクティビティを探す

ランタイムポリシーを作成・維持して、CI/CDやレジストリのスキャンでは検出されなかった脅威や攻撃をブロックできるようにする必要があります。

脅威検知

Sysdigは、CNCF Falcoプロジェクトのオープンソース検出エンジンを活用して、ホストやコンテナ上の異常なアクティビティをランタイムで監視します。また、AWS CloudTrailのログや、KubernetesやEKSが管理するサービスを使用している場合は、オーケストレーションレイヤーからアクティビティを取り込み、監視します。



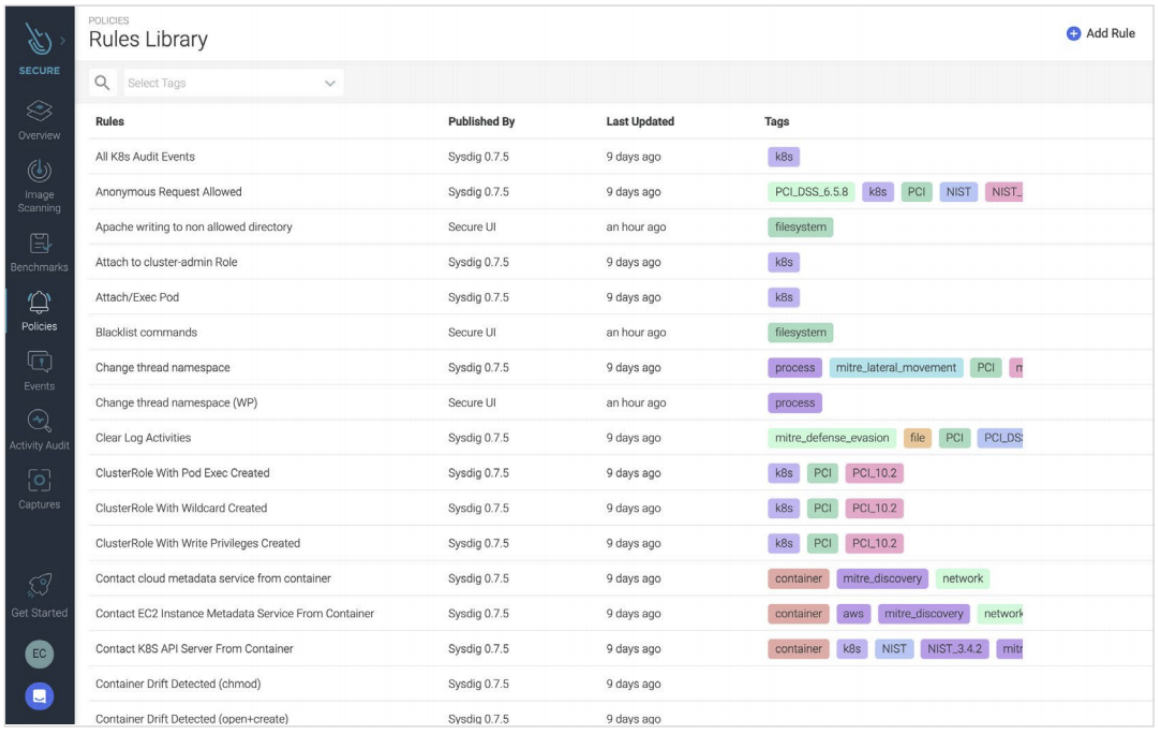
EKSからのKubernetesサーバーAPIイベントの取り込みについては[こちら]をご覧ください。

CI/CDプロセス中に一度だけコンテナをスキャンしたり、AWS Elastic Container Registryからスキャンするだけでは十分ではありません。既知のソフトウェアの脆弱性は検出されますが、いくつかのセキュリティ脅威は、その性質上、ランタイム時にのみ顕在化するものです。

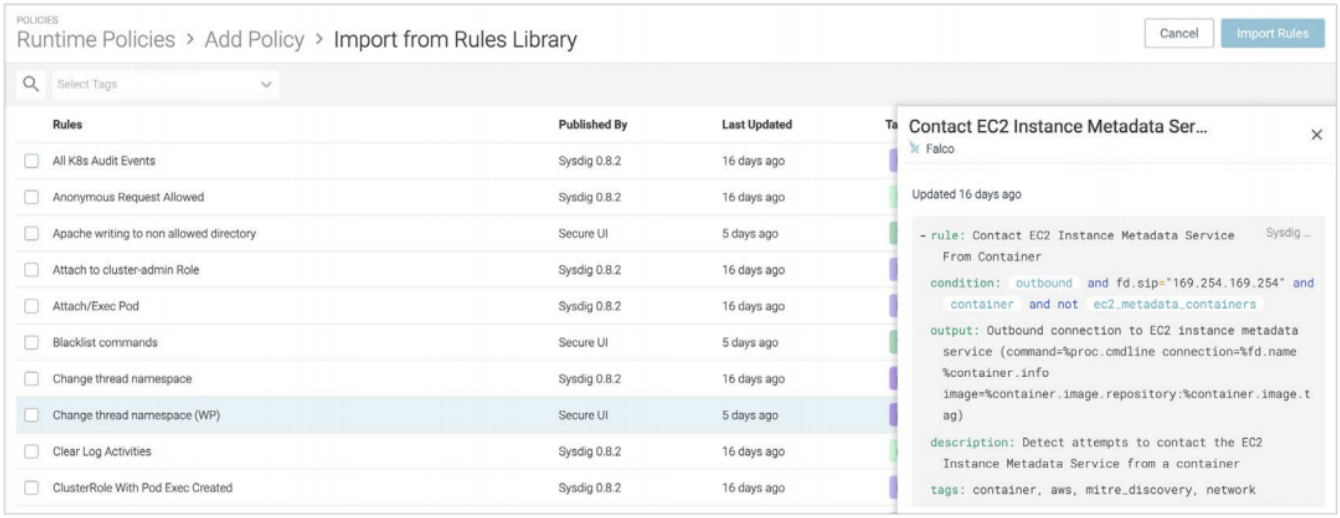
- ゼロデイ脆弱性や自社ソフトウェアに特有の非公開の脆弱性
- 不安定な動作やリソースの漏洩を引き起こすソフトウェアのバグ
- 内部での権限昇格の試みや、隠れた/埋め込まれたマルウェア

60種類以上のデフォルトのランタイムセキュリティポリシーがSysdig Secureライブラリを通じてすぐに利用でき、ランタイムセキュリティを簡単に実装して脅威を検出することができます。これには以下が含まれます。

- 規制されているコンテナコンプライアンス基準に対応したコンテナランタイムセキュリティポリシー：NIST SP 800-190、PCI、CIS、またはMITRE ATT&CKフレームワーク。
- 最も広く普及しているコンテナ攻撃のランタイム検知：クリプトマイニング、シークレットの流出、コンテナの隔離違反、ラテラルムーブメントなど。
- 予期せぬプロセスアクティビティ、アウトバウンド接続、ターミナルシェルセッションなどのセキュリティ監視。

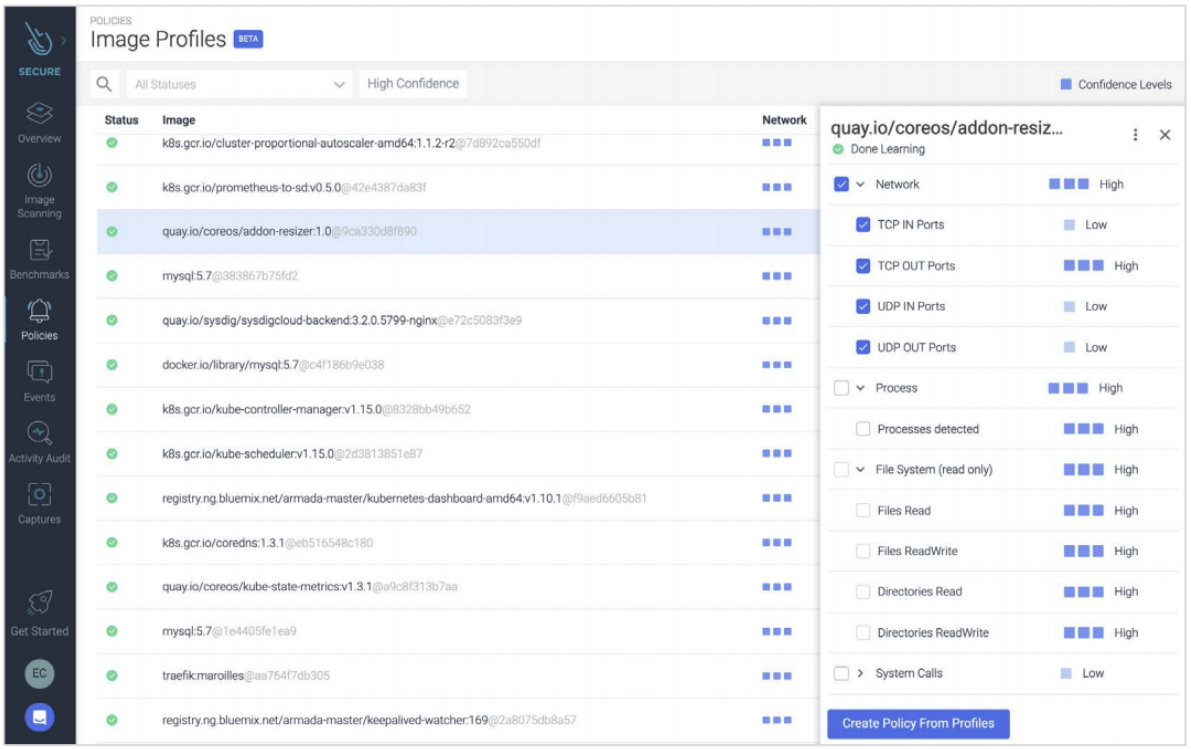


オープンソースのFalcoを採用した拡張可能なポリシーエンジンにより、運用チームやセキュリティチームは、ビジュアルインターフェースを介して独自のルールをカスタマイズしたり記述したりして、要件に合ったきめ細かなポリシーを構築することができます。コミュニティによって作成されたFalcoルールは、Cloud Native Security Hubで利用できます。



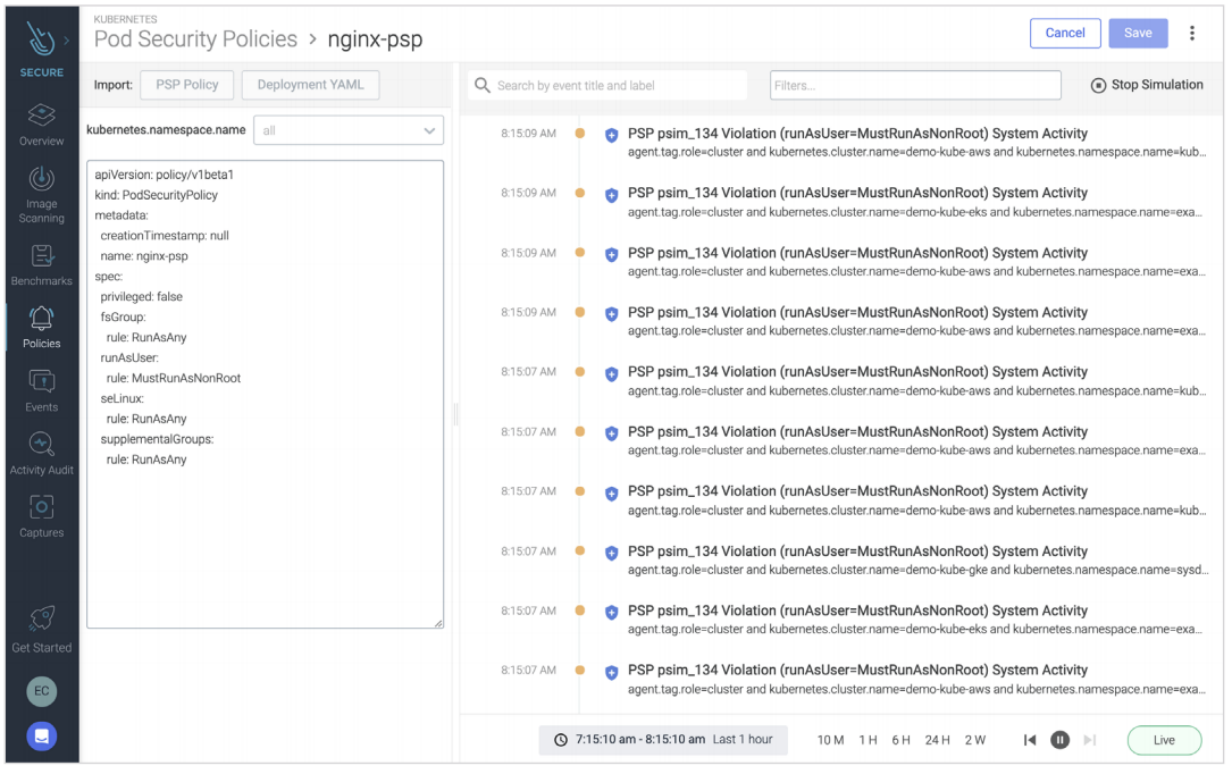
ランタイムイメージプロファイリング

大規模環境におけるランタイムセキュリティの構築と維持の負担を軽減するために、Sysdig Secureはランタイムイメージプロファイリング機能を備えています。イメージプロファイリングは、コンテナランタイムの動作を自動的にモデル化、分析、学習して、包括的なコンテナランタイムプロファイルを作成し、自動的にポリシーを構築します。これには、kubeapiserverのアクティビティやsyscallを分析し、ECS、EKS、クラウドラベルなどの様々なメタデータでリッチ化することが含まれます。このアプローチにより、機械学習による異常検知が強化され、脅威が伝播する前にブロックすることができます。



Kubernetesのネイティブコントロールによる脅威の防止

Sysdigは、ポッドセキュリティポリシー（PSP）など、Kubernetesのネイティブコントロールを用いて脅威を防ぎます。Kubernetes Policy Advisorは、PSPの生成を自動化し、デプロイ前に検証することで、PSPを適用した際にアプリケーションが破損しないようにします。これにより、ユーザーは本番環境でPSPを迅速かつ容易に採用することができます。また、PSPはKubernetesネイティブの制御メカニズムを提供し、ホスト上のすべてのアクションを傍受しなければならないエージェントとは異なり、パフォーマンスに影響を与えることなく脅威を防ぐことができます。Sysdig Secureは、PSPのようなKubernetesネイティブなコントロールをエンフォースメントに活用しています。詳細はブログ Pod Security Policies in production with Sysdig's Kubernetes Policy Advisor でご覧いただけます。また、Sysdigのランタイムセキュリティ機能についてはこちらをご覧ください。



Sysdig Secureを使用することで、運用チームやセキュリティチームはコンテナのセキュリティポリシー作成の負担を軽減し、ボンネット内で何が起こっているかをより詳細に管理することで、より高い透明性と保証を得ることができます。

AWS クラウド セキュリティ ポスチャーマネジメント

Sysdig社が実施した脅威に関する調査によると、クラウド、ワークロード、コンテナを一元的に把握することで、セキュリティ侵害の大半で使用されている一般的な手法であるラテラルムーブメント攻撃の検知と対応の両方にかかる時間を短縮することができます。

異なるクラウドとコンテナのセキュリティツールを使用すると、セキュリティ侵害を完全に理解し、影響を受けたシステムを明らかにするために、異なるデータソースを手動で相関させる必要があるため、セキュリティオペレーションが複雑になります。Sysdigは、クラウドセキュリティポスチャーマネジメント（CSPM）やクラウドの脅威検知と、コンテナやKubernetesのセキュリティ機能を含むクラウドワークロード保護を単一のプラットフォームでペアリングします。

インシデントのタイムラインを統一し、リスクベースのインサイトを追加することで、SysdigはAWSクラウドサービスやコンテナにおける脅威の検知にかかる時間を数週間から数時間に短縮します。クラウド開発チームは、攻撃者がどこからスタートし、環境内を移動する際の各ステップを正確に把握することができます。

クラウドアセットディスカバリー

クラウドアセットは境界の制限を受けずに動作します。また、リソースはAPIやその他のコネクターを通じてAWS環境に継続的に持ち込まれるため、どのアセットが実際に環境と相互作用しているかを知る必要があります。企業は、AWS環境全体にセキュリティを適用するために、これらすべてのデータソースがどのように接続され、相互作用しているかについてのインテリジェンスを含む、アセットのインベントリーを必要としています。

AWSのアプリケーションは通常、特定の機能を実行する複数のサービスで構成されており、APIを通じてアクセスできます。各サービスには、クラウド環境内の他のリソースへの接続があります。これらのリソースには、オブジェクトストア、マイクロサービス、データベース、S3バケット、その他のリポジトリやリソースが含まれます。

ほとんどの組織では、これらのリソース、その関係、および構成を特定するために手動のアプローチを適用しています。継続的に拡大・縮小する環境での手作業による管理はスケーラブルではないため、これらのアセットとその動作のインベントリーを作成・追跡するための自動化されたサービスが必要となります。

AWSが提供するのは...

AWS Application Discovery Servicesは、オンプレミスのサーバーやその他のクラウドアセットの使用状況や構成データを収集します。AWS Migration Hubと統合されており、統合または別の形で環境に入ってきた新しいアセットを即座に識別することができます。Application Discovery Services APIを使用すると、ユーザーは検出されたすべてのサーバーのシステムパフォーマンスと利用率のデータにアクセスできます。

Application Discovery Service APIを使用すると、検出されたサーバーのシステムパフォーマンスと利用率のデータをエクスポートできます。このデータをコストモデルに入力して、それらのサーバーをAWSで稼働させた場合のコストを計算します。また、サーバ間のネットワーク接続に関するデータをエクスポートすることができます。この情報は、サーバ間のネットワーク依存関係を判断し、移行計画のためにアプリケーションにグループ化するのに役立ちます。

Sysdigが追加するのは...

クラウドセキュリティチームは、Sysdigを使って、AWSクラウド環境で稼働しているシステム、アプリケーション、サービス、スクリプトを自動的に検出し、セキュリティ体制を管理することができます。これにより、アカウント、VPC、リージョン、S3バケット、RDSなどのクラウドアセットをマッピングし、センシティブなデータ（顧客データ、コンプライアンス規制の対象となるデータなど）がどこに保存され、処理されているかをより深く理解することができます。

この機能は、クラウドインフラのセキュリティを確保するためのオープンソースツールであるCloud Custodianをベースにしており、お客様のAWSアカウントで運用されているリソースやアセット、各リソースやプロジェクトに組み込まれているすべてのアセットをリアルタイムでダッシュボードに表示します。現在の運用状態のベースラインを把握することで、最も重大な脅威が存在するサービスをより優先的に選択し、修復を加速することができます。

Sysdigでは、各AWSリソースやプロジェクトを掘り下げて、対応する設定を確認することができます。Sysdigは、AWSアカウント内のアセットを特定し、他のシステムからのデータと合わせて分類することで、クラウド内のすべてのサービスについて1つの真実の情報源を作ります。

アセット管理は、コンフィギュレーションコンプライアンスの重要な要素です。クラウド環境は動的で複雑です。構成や変更を手動で追跡・検出することは不可能です。Sysdigは、PCI-DSSやNIST 800-53のガイドラインをAWS環境のアセットにマッピングし、構成がこれらの特定のコンプライアンスフレームワークの要件を満たしていない場合、継続的にチェックし、アラートを提供します。

Sysdigのユーザは、インベントリ管理で提供されるすべてのデータをカスタマイズすることができ、イベント情報を手動で関連付ける必要性を減らすことができます。Sysdig SecureはKubernetesのアクティビティに関する関連情報も提供するため、AWSマネージドクラウドサービスのセキュリティイベントと並行して、ワークロードで何が起こっているのかをより深く理解することができます。

静的コンフィギュレーション管理

アプリケーションをはじめとするクラウドベースのシステムがセキュリティを重視して設計されていても、クラウド環境の変化に伴い、当初設定した設定や構成が適切でなくなることがあります。その結果、脆弱性が顕在化したり、本番アプリを監視する設定がセキュリティ上のリスクになったりすることがあります。そこで重要なのは、構成管理をAWSリソースに適用することで、特定の規制フレームワークへのコンプライアンスを確保するだけでなく、組織のAWSアカウントに対応するセキュリティ態勢を維持することです。

クラウドのワークロードとアプリケーション開発が急速に変化する中で、アプリの機能は継続的に進化します。その結果、手動では追跡できない構成変更が発生します。AWSにおいてSysdigを活用すると、クラウド利用者は、AWSアカウント全体の継続的なクラウド構成監視と監査レポートの恩恵を受けることができます。これにより、AWSインフラストラクチャーのネットワーク、ストレージ、ユーザ・アクセス、ログの各側面におけるコンプライアンス違反の検出が出来るようになります。

AWSが提供するのは...

AWS Configは、AWSリソースの構成に関する継続的な評価、監査、およびレポートを行います。環境のAWSリソースの構成を監視してログを記録し、変更が必要な場合は事前に定義された構成を適用することができます。管理者は、構成の変更と、その変更が他のAWSリソース間の関係にどのような影響を与えるかを確認することができ、変更の履歴を分析することができます。ユーザーは、自分のワークロードが一定期間内にどのような構成で動作していたかを確認し、いつ（環境内のどこで）AWSリソースの変更が構成に影響を与えたかを判断することができます。

AWS Configは有効にすると、指定されたアカウントに存在するサポートされたAWSリソースを検出し、各リソースに対して受け入れられた構成レポートを生成します。AWS Configは、ユーザの環境でサポートされているすべてのリソースに対して構成アイテムを作成します。

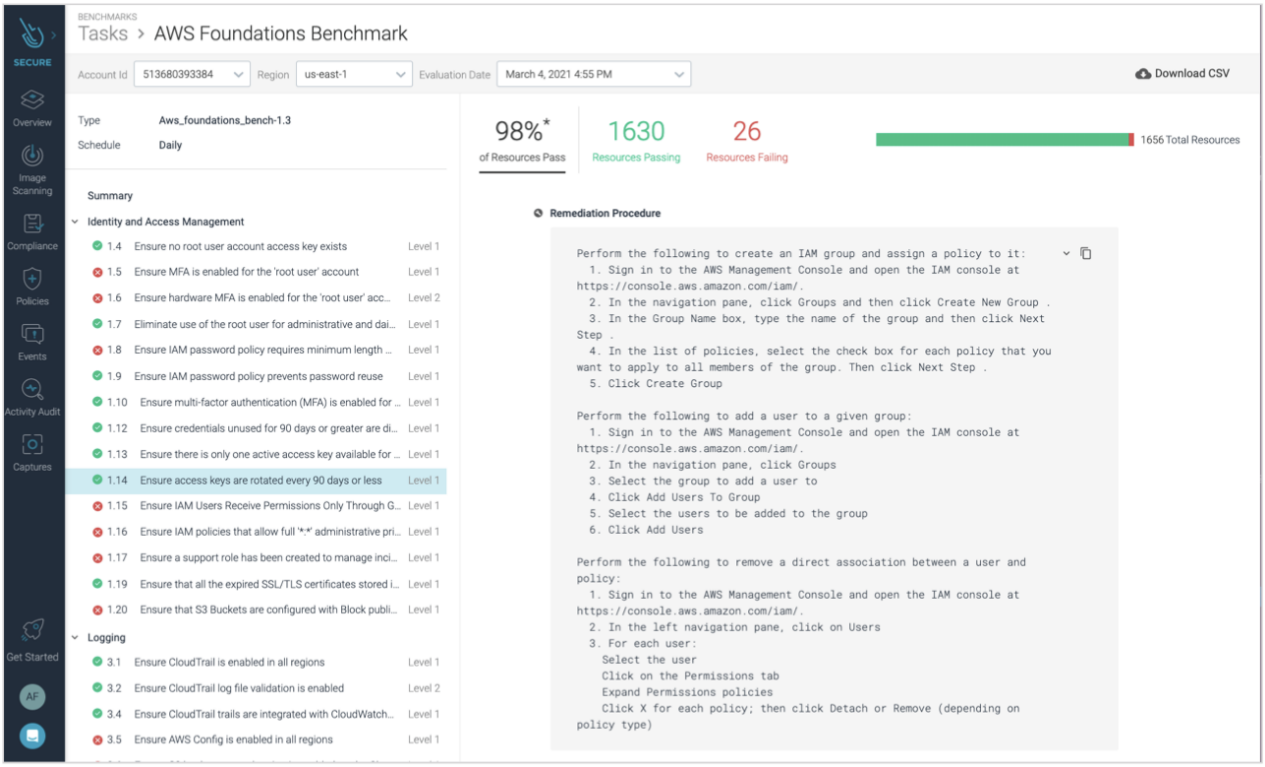
Sysdigが追加するのは...

AWSアカウントでは、より多くのワークロードや増加するアプリケーション間の統合が行われるため、イベントや運用の証跡の量が圧倒的に多くなります。スケーラブルで自動化されたアプローチがなければ、分析は不可能です。Sysdig Secureは、リスクのある構成設定を特定し、クラウドやコンテナ環境の現在のセキュリティ態勢を可視化するのに役立ちます。これにより、パブリックストレージ

バケット、公開されたセキュリティグループ、漏洩したシークレット/クレデンシャルなどの誤設定の検出が簡素化され、コンフィギュレーションドリフトがあるかどうかを迅速に判断することができます。

Sysdigは、お客様のクラウド構成をAWS Foundations CISベンチマークと比較して定期的に分析します。これは、お客様のAWSアカウントのチェック項目をまとめたもので、どのサービスや構成にセキュリティ上の課題があるかをお知らせします。これにより、どのサービスや構成がセキュリティ上の課題となっているかがわかります。また、クラウドアセットの構成上の問題を修正するための適切な手順を示すガイダンスも提供されます。

セキュリティチームやDevOpsチームの観点から見ると、Sysdigは構成に関する洞察を読みやすく文脈に沿った形式で提供し、監査を支援することで、コンプライアンスやポリシーの遵守を簡素化し、具体的なビジネスメリットをもたらします。これは、自動化された方法で目標を達成することができるため、セキュリティチームにとってますます不可欠なタスクとなっています。



AWS CloudTrailのログによる脅威の検知

AWS CloudTrailは、AWS環境のガバナンスとコンプライアンス監査を可能にするネイティブサービスです。ユーザー、ロール、またはAWSサービスのアクションはCloudTrailのイベントとして記録されます。これには、AWSマネジメントコンソール、AWSコマンドラインインターフェイス、およびAWS SDKとAPIに対するあらゆる変更が含まれます。

AWSが提供するのは...

CloudTrailから得られるイベント履歴は、セキュリティ分析、リソース変更の追跡、トラブルシューティングを簡素化します。CloudTrailが提供する情報を利用して、お客様のAWSアカウントにおける異常な活動を検知し、運用分析やトラブルシューティングを簡素化することができます。CloudTrailは、お客様のAWSリソースのセキュリティを脅かすアカウントアクティビティの追跡と対応を可能にします。

また、AWSのワークロード、アカウント、APIコール、S3バケットに格納されたデータにおける悪意のあるアクティビティや異常な動作を監視する脅威検知サービス「AWS GuardDuty」を活用することもできます。このサービスは、CloudTrailからの監査ログを頼りに、セキュリティ上の問題を示唆するような異常なアクティビティを特定します。

Sysdigが追加するのは...

インフラの成長に伴い、CloudTrailから取得できるイベントや運用ログの量は、手動での分析や対応が不可能なサイズにまで増加する可能性があります。脅威への対応が遅れると、大きな影響を及ぼす可能性があります。

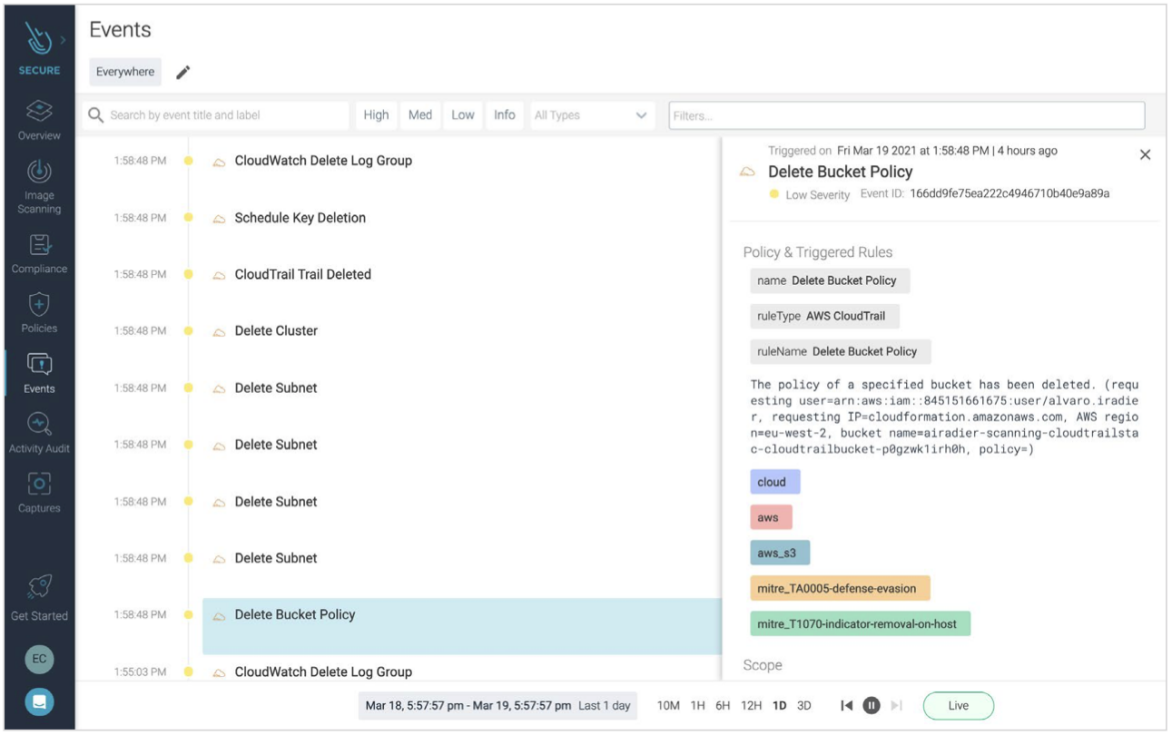
Sysdigは、コンテナやKubernetesのデプロイメント全体の脅威を検知するのと同じエンジンであるオープンソースのFalco脅威検知をベースにした柔軟なセキュリティルールを使用することで、CloudTrailイベントの評価をリアルタイムで自動化するという課題を解決します。

SysdigとCloudTrailの統合により、事前に設定されたポリシーを使用したり、独自の検出を作成して予期せぬアクティビティを警告することもできます。100以上のコミュニティ主導の、すぐに使えるFalcoルールの包括的なセットを活用することで、時間を節約することができます。さらに、DevOps

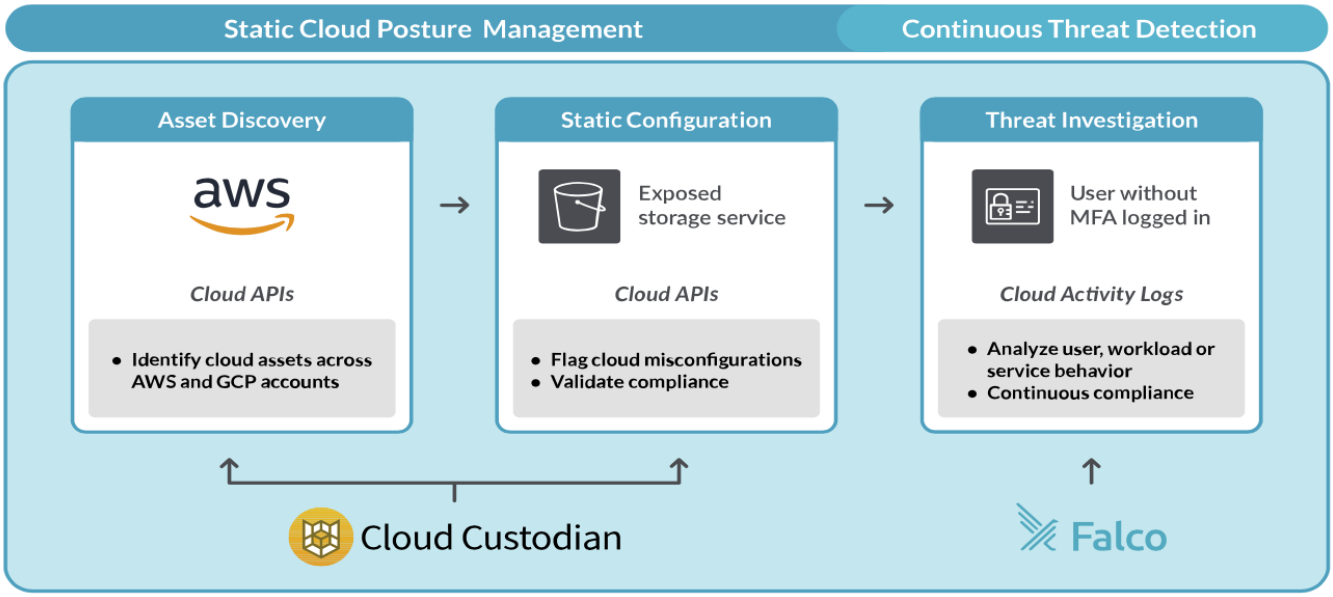
とセキュリティチームは、AWS環境を離れることなく、AWS Security Hubでイベントを直接確認することで、発見を素早く得ることもできます。

一度設定すれば、Sysdig Secureは、お客様のすべてのクラウドアカウントのIAM、RDS、EC2、RedShift、VPCなどのサービスについて、不審なクラウドアクティビティやイベントを継続的に検出し、報告します。ここでは、いくつかの使用例をご紹介します。

- 不審なIAMアクティビティや異常なパーミッション変更を探す。
- プロセスの実行パターンを検出し、予期せぬ動作やリモートコードの実行を検出する。
- クレデンシャルの盗難、特に有効期限の長いクレデンシャルや高権限のクレデンシャルの盗難を確認する。
- クラウドリソース（S3など）、仮想サーバのインフラポート、コンテナ、コンテナオーケストレーションプラットフォームの構成の変更を特定する。
- 意図しない情報の露出による機密データの漏えいを特定する。
- 過去のインシデントのデータを調査し、パターンを検出する。



AWSのウェブサイトでは、CloudTrailがサポートするサービスの一覧を見ることができます。



AWSコンテナサービスの監視

コンテナは短命で、ダイナミックで、常に変化しています。コンテナが死ぬと、中のものはすべてなくなります。SSHやログを見ることもできませんし、モノリシックなアプリケーションに使われてきた従来のツールのほとんどは、何か問題が起きたときにはほとんど役に立ちません。コンテナは、アプリケーションをパッケージ化して分離し、どこにでも一貫してデプロイできるので、運用には最適です。

しかし同時に、トラブルシューティングが困難なブラックボックスになってしまいます。

コンテナベースのアプリケーションの動的な性質を監視することは、クラウドサービスの高可用性とパフォーマンスにとって重要です。コンテナ上で動作するマイクロサービスアーキテクチャーは、アプリケーションの拡張性と開発速度を向上させ、イノベーションの迅速化と新機能の市場投入までの時間短縮を可能にします。しかし、アプリケーション内のマイクロサービスの数が増えると、これらの環境内の可視性を確保することが難しくなります。マイクロサービスベースのアプリケーションは、複数のインスタンスに分散させることができ、コンテナは必要に応じてマルチクラウドのインフラを移動することができます。Kubernetesのオーケストレーションの状態を監視することは、Kubernetesがすべてのサービスインスタンスを稼働させ続けているかどうかを理解するための鍵となります。

AWSが提供するのは...

AWSが提供するAmazon CloudWatchは、ログ、メトリクス、イベントを通じてAWSリソースやアプリケーションの運用状態を監視・観測するサービスです。

CloudWatchは、アプリケーションの監視、システム全体のパフォーマンスの変化への対応、リソース利用の最適化、運用の健全性を統一的に把握するためのデータと実用的なインサイトを提供します。CloudWatchは、ログ、メトリクス、イベントの形で監視および運用データを収集し、以下のようなAWSリソース、アプリケーション、サービスの統一的なビューを提供します。

AWSリソース、アプリケーション、サービスを一元的に把握することができます。CloudWatchは、環境における異常な動作の検出、アラームの設定、ログとメトリクスの並べての視覚化、自動化された

アクションの実行、問題のトラブルシューティング、アプリケーションをスムーズに動作させるためのインサイトの発見などが可能です。

また、PrometheusのメトリクスをCloudWatchで収集することで、アプリケーションパフォーマンスの低下や障害の監視、トラブルシューティング、アラートを迅速に行うことができます。

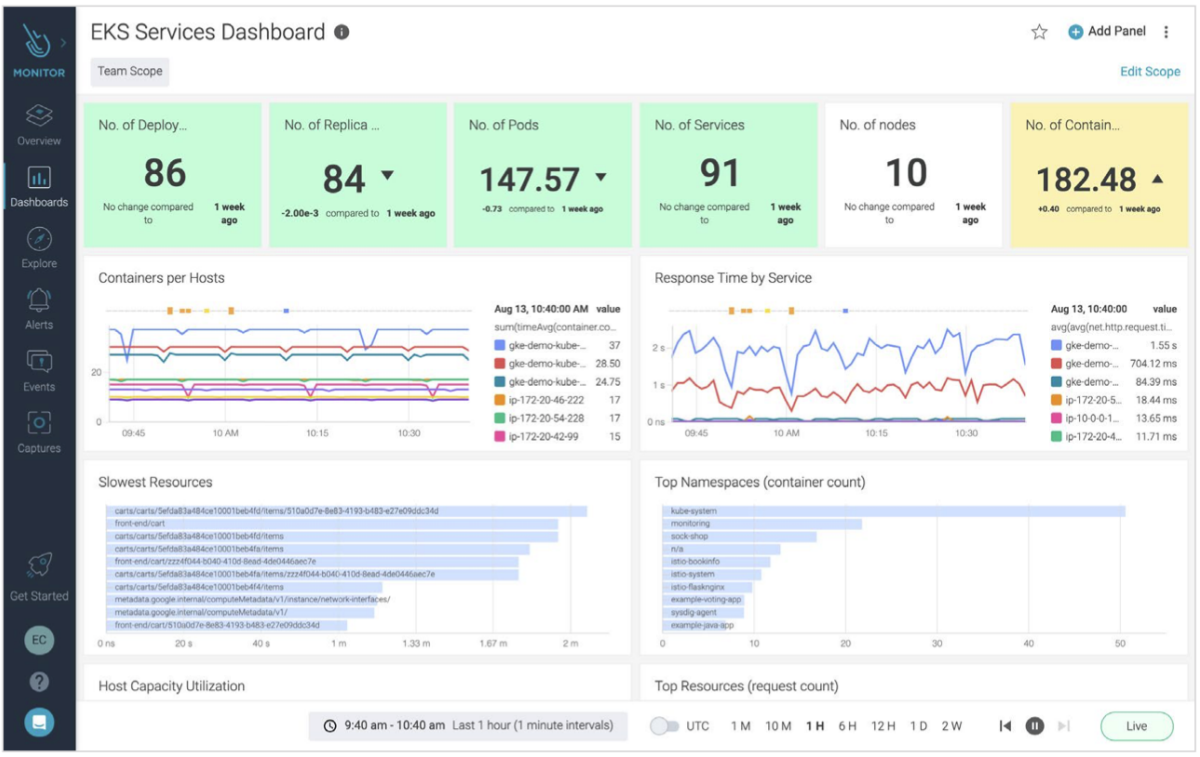
Sysdigが追加するのは...

Sysdig Monitorは、クラウドインフラストラクチャー、サービス、アプリケーションのパフォーマンスと可用性を最大化します。Prometheusとの完全な互換性を備えた大規模なクラウド監視を実現し、急速に変化するコンテナ環境に深い可視性を得られます。クラウドとKubernetesのコンテキストで強化されたシステムコールから得られる粒度の細かいデータを使用することで、問題を迅速に解決することができます。また、ハイブリッドおよびマルチクラウドのモニタリングのために、チーム間でデータを統合することで、サイロを取り除くこともできます。

Kubernetesとコンテナにおける監視

Sysdigは、クラスター、デプロイメント、ネームスペース、ワークロードのゴールデンシグナルを含む、自動アラートと詳細な健全性およびパフォーマンス情報をクラウドチームに提供します。クラウドとKubernetesのコンテキストで強化されたコンテナアクティビティの深い可視性により、チームは複雑なコンテナデプロイメントを管理することができます。これにより、以下のことが可能になります。

- インフラストラクチャー、サービス、アプリケーションに対する深い可視性により、健全性とパフォーマンスを監視する
- Kubernetesオーケストレーションのコンテキストを用いて、クラスターの運用状況を可視化する
- コンテナとクラウドのコンテキストを使用して、問題解決のためのオーナーを即座に特定
- 過剰なリソースを消費しているポッドを特定し、キャパシティの上限を監視
- アプリケーションのオートスケーリングの動作を監視し、予期せぬ課金を抑制します
- クラスターやクラウド全体のキャパシティを最適化してコストを削減



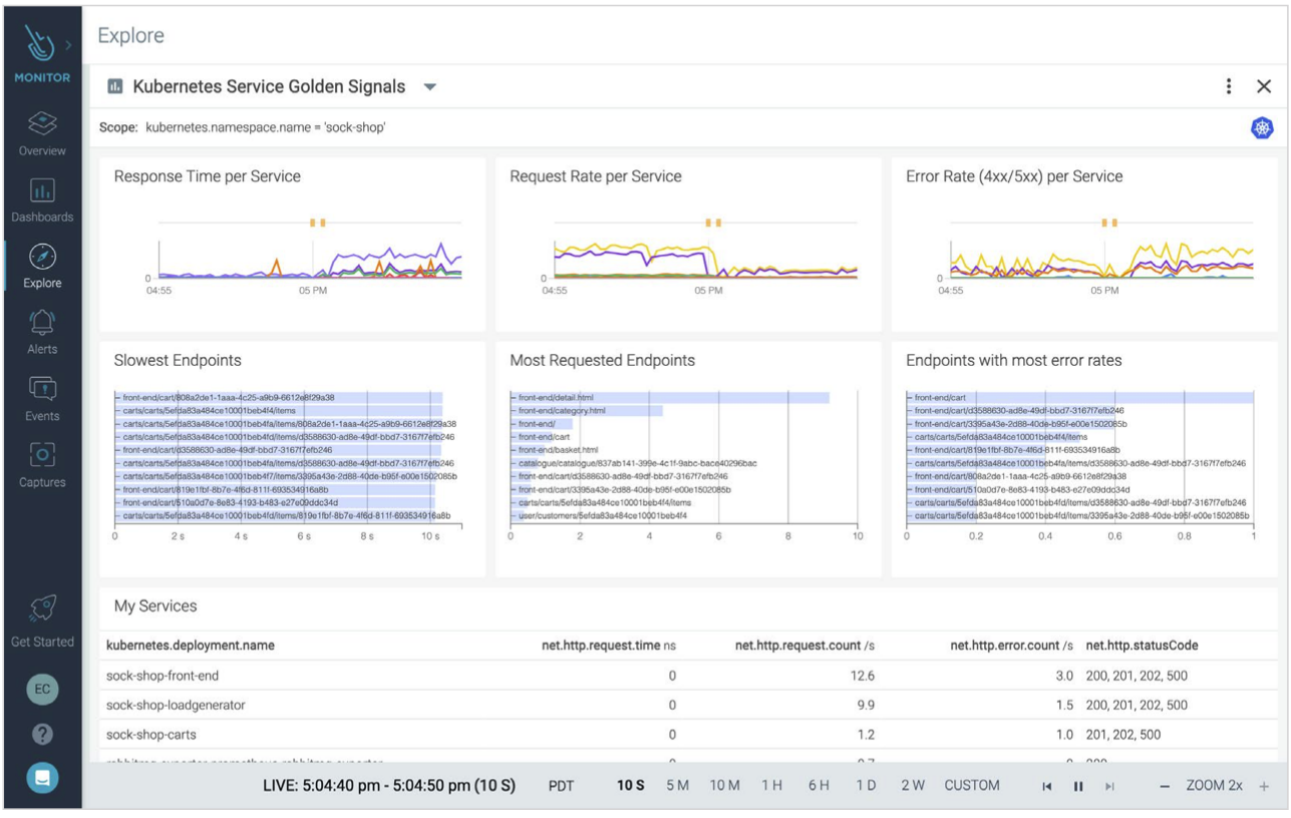
アプリケーションとサービスの監視

レイテンシー、エラー、トラフィック、サチュレーションの各メトリクスは、サービスの健全性を監視するための[ゴールデンシグナル]として知られています。これらのメトリクスは、サービスを利用するユーザーから見た、アプリケーションの実際の健全性とパフォーマンスを示します。本当に重要なものを見て、アプリケーションの本当の問題を隠してしまうような罠を避けることで、時間を節約することができます。

Sysdig Monitorは以下のことを可能にします：

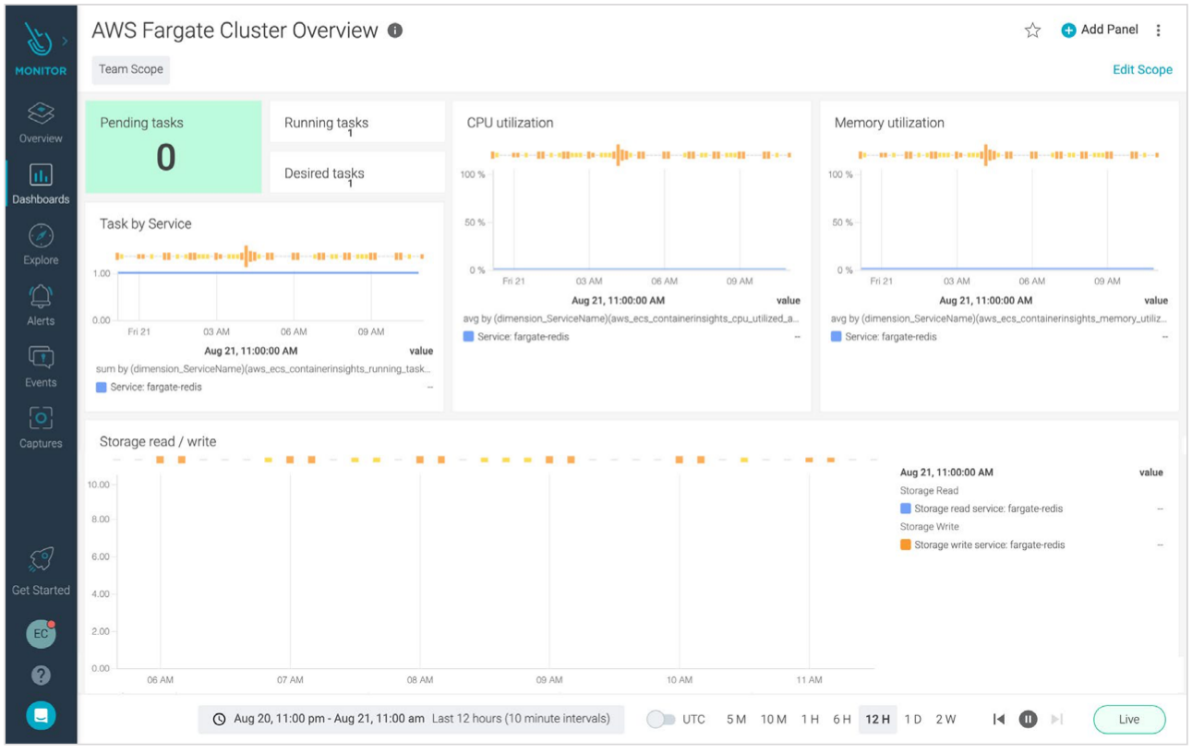
- アプリケーションの可用性とセキュリティに関する情報を一元管理することで、問題解決までの時間を短縮します。
- アプリケーションのパフォーマンスを向上させ、Kubernetesやクラウドのコンテキストで強化された詳細なコンテナの可視性ときめ細かなメトリクスにより、問題を迅速に解決します。

- クラウドサービスやデータベースなど、AWS環境の主要なコンポーネントのメトリクスを、すぐに使えるダッシュボードで確認できます。
- 特定のセキュリティインシデントがユーザーへのサービス提供に与える影響を監視することができます。
- チーム、SSO、RBACなどのエンタープライズグレードのアクセス制御を監視システムに利用することで、リスクを低減します。
- クラウドスケールでのPrometheusとPromQLの完全な互換性により、既存の開発者の投資を活用します。
- Prometheusと互換性のあるエクスポーター、ダッシュボード、アラートを使用して、何百ものアプリケーションやサービスにモニタリングを拡張します。
- PromCat.ioが提供するKubernetesプラットフォームやクラウドネイティブサービスのための、精選され、文書化され、サポートされた監視統合を使用することで、生産性を高めることができます。



Sysdigは多くのAWSサービスをネイティブにサポートしており、PrometheusとAmazon CloudWatchの併用も容易になります。Sysdig Monitorは、Prometheus経由でAWS CloudWatchのメトリクスを抽出し、あらかじめ構築されたSysdigやGrafanaのダッシュボードを使って可視化します。エンタープライズクラスのPrometheusモニタリングのためのオープンソースのリソースカタログである[Promcat.io]では、AWSサービスのための吟味されたPrometheusエクスポーター、ダッシュボード、アラート、およびレコーディングルールの精選されたリポジトリを利用できます。

ドキュメントによる検証済みのサポートがあれば、Prometheusインテグレーションの調査やメンテナンスに費やす開発者の時間を減らし、何週間もの労力を節約することができます。AWSインテグレーションの例としては、AWS Fargate、AWS Lambda、AWS Application Load Balancer (AWS ALB)、AWS Elastic Load Balancer (AWS ELB)、Amazon Simple Storage Service (Amazon S3)のサポートがあります。



サービスメッシュにおける可視性

マイクロサービスの管理を効率化し、運用を容易にするために、Istio、Linkerd、AWS App Meshなどのサービスメッシュソリューションが、コンテナ上に構築されたマイクロサービスインフラの次のコアビルディングブロックとなっています。サービスメッシュは、サービスディスカバリー、認証、ロードバランシング、暗号化、トレースなどの機能により、コンテナ化されたマイクロサービスをより効率的に大規模に実行、管理、監視するのに役立ちます。

AWSが提供するのは...

AWS App Meshは、ECS、EKS、Fargate向けのマネージドサービスメッシュプラットフォームです。AWS上で動作するマイクロサービスを簡単に監視・制御することができます。App Meshは、マイクロサービスの通信方法を標準化し、ユーザーにエンドツーエンドの可視性を与え、アプリケーションの高可用性を確保します。App Meshは、コードを変更することなく、アプリケーション内のマイクロサービス間のすべての通信に対して、単一のビューとコントロールポイントを提供します。

AWS App Meshは、オープンソースのEnvoyプロキシを使用しているため、マイクロサービスを監視するためのAWS Partner Network（APN）やオープンソースのツールと幅広く互換性があります。

Sysdigが追加するのは...

SysdigはAWS App Meshをサポートし、AWSコンテナサービス上で動作するマイクロサービスのパフォーマンスを可視化し、サービスメッシュのセキュリティプロファイルや全体的な健全性をさらに把握することができます。Sysdigは、AWS App Meshのユーザーがサービスメッシュのパフォーマンスを監視し、インフラストラクチャー全体のパフォーマンスとセキュリティのメトリクスを表示することで、コンテナ化された環境にさらなるコントロールを与えることができます。

Sysdigは、EnvoyプロキシのPrometheusエンドポイントからメトリクスを自動的にスクレイピングする機能により、AWS App Meshのモニタリングを強化します。これにより、企業はEnvoyからのメトリクスを安全に収集し、警告を発し、可視化することができます。収集されたデータは、SysdigがKubernetesを含むコンテナインフラ全体から収集して充実させた膨大なメトリクスやイベントデータと相関させます。

コンテナフォレンジックとインシデント対応

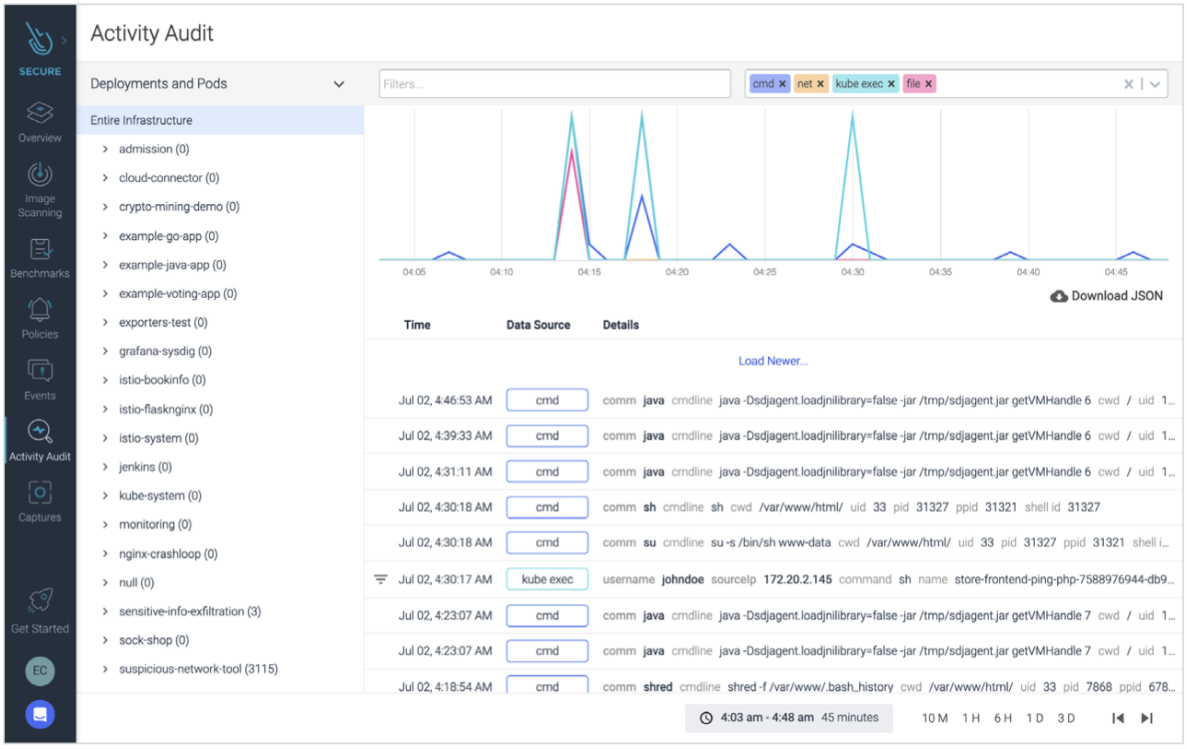
問題のトラブルシューティングやセキュリティインシデントの事後分析を行う際、典型的な課題の一つは、コンテナが破壊されると、関連する情報がすべて消えてしまうことです。

EKSやECSのようなコンテナソリューションでは、このようなことは常に起こります。コンテナはノード間で移動することができ、サービスはスケールアップ/ダウンしてコンテナインスタンスを削除します。問題の根本的な原因を特定し、問題が悪意のある行為から来ているのか、それともアプリの設定ミスから来ているのかを認識できなければなりません。

CloudWatchは、ログ、メトリクス、イベントを使用して洞察を提供しますが、動的コンテナのトラブルシューティングのために作られたものではありません。コンテナは一過性のものであるため、コンテナがなくなった後にセキュリティインシデントで何が起こったかを分析することは困難です。侵入者が行った手順をどうやって再現するのか？どうやってアクセスしたのか？影響はどうでしたか？何かマルウェアをインストールしたのか？データは流出しましたか？攻撃の範囲はどこまで広がったか？

Sysdigが追加するのは...

SysdigのActivity Auditは、インシデントレスポンスの迅速化とKubernetesの監査を可能にします。Sysdigは実行されたコマンド、ネットワーク、Kubernetesのアクティビティをキャプチャーし、相関させることで、SOCチームは何が起こったのかを見極めることができます。Sysdigのキャプチャーを使えば、生成されたプロセス、ネットワーク接続、ファイルシステムのアクティビティなど、すべてのコンテナのアクティビティを詳細なレベルで記録することもできるので、コンテナがなくなった後でもイベントを詳細に理解し、Kubernetesのフォレンジックを行うことができます。



詳しくは[Sysdig Activity AuditによるKubernetesでのインシデント対応]をご覧ください。

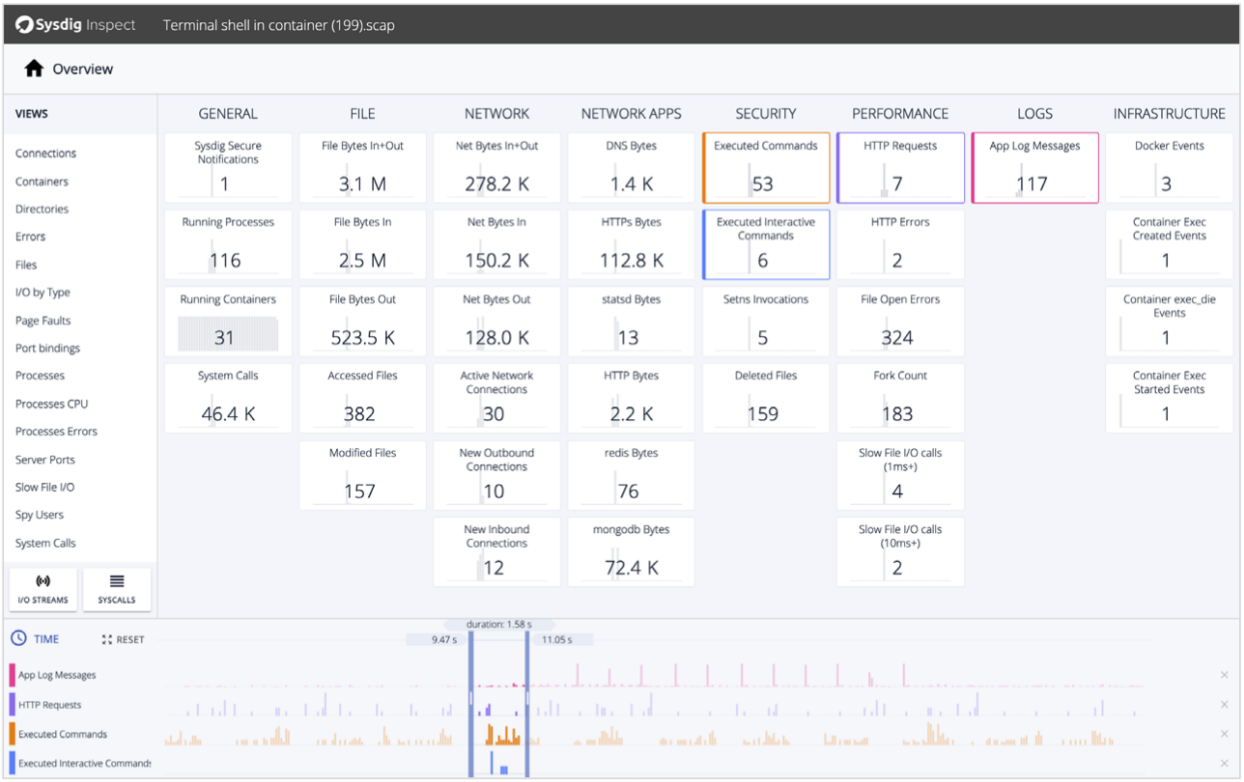
Sysdigは、アラートチャンネル、AWS SNS、またはSIEMに通知を配信します。これにより、コンテナ環境全体のセキュリティ調査結果を統合することができ、セキュリティアラートの表示や管理、AWSアカウント全体のコンプライアンスチェックの自動化が可能になります。Sysdig SecureとFalcoは、FalcoとAWS Firelensによる[マルチクラスタセキュリティ on EKS & ECS]で見られるように、FireLensを通じてCloudwatchにイベントを送信します。

Sysdigを使えば、セキュリティチームはポッド内の問題を解決し、AWSコンテナサービスのアプリケーションコンテキストに関連したシステムアクティビティを再構築してフォレンジックを行うことができます。

Sysdigが追加するのは...

- 詳細なフォレンジックレポートにより、あらゆるセキュリティ侵害の影響を迅速に把握し、抑制することができます。

- 詳細な活動記録により、何が起こったのかを迅速に判断し、インシデント対応を合理化します。Falcoルールライブラリを活用したきめ細かなポリシーにより、ランタイムのポリシー違反を分析、監査します。ファイルアクティビティ、ネットワークトラフィック、アプリケーションプロトコル、コマンド、ログ、またはイベントなど、侵入時の手順を簡単に再現できるので、データの流出やラテラルムーブメントなどのインシデントを調査することができます。これにより、迅速に復旧し、今後の防御を強化することができます。
- 本番環境外のコンテナでの事後分析を行う事ができるため、AWSコンテナサービスのコンテナポッドがなくなった場合でも、フォレンジックキャプチャーを分析し、すべてのシステムアクティビティを再現することができます。



AWSとSysdig Secure DevOps Platformとの連携強化

SysdigとAWSは、お客様がワークフローを容易に移行し、AWSのコンテナやクラウドサービス上に構築されたアプリケーションに移行できるように設計された、長いパートナーシップを結んでいます。Sysdigを使用すると、企業はクラウドが最適化された機能を活用できるようになります。つまり、迅速な開発とデリバリー、継続的なイノベーション、ビジネスとテクノロジーの運用の拡大、資本コストを変動コストへ、そして必要なセキュリティと ユーザー、データ、およびリソースを保護するために必要なセキュリティと可視性の確保など、クラウドが最適化された機能を活用する能力を企業に提供します。

Sysdig Secureは、AWSの共有責任モデルの一部を維持するための、即時かつ包括的なクラウドセキュリティを提供します。Sysdig Secure DevOps Platformは、AWSコンテナサービス上でコンテナワークロードを実行しているDevOpsチームとクラウドチームが、セキュリティをワークフローに組み込み、パフォーマンスと可用性の可視性を得て、コンテナを監視し、コンプライアンス要件を実装することを可能にします。

Sysdigは、AWSパートナーネットワーク（APN）のAWSアドバンストパートナーとして、コンテナセキュリティ、監視、DevOpsのコンピテンシーを持って、これらの統合をサポートしています。私たちの目標は、お客様がAWS上であらゆるワークロードを安全に実行できるようにすることです。

開発者、プラットフォーム運用、セキュリティチームがクラウドアプリケーションを構築する際に留意しなければならないのは、いくつかの異なるセキュリティと監視のレイヤーです。以下の表は、これらのレイヤーをまとめたもので、AWSコンテナサービスの機能と、Sysdig Secure DevOps Platformを活用してコンテナとKubernetesのセキュリティ、コンプライアンス、監視をさらに強化することで得られる共同のメリットを紹介しています。

コンテナプラットフォーム

プラットフォーム	AWSソリューション	Sysdig+AWSのベネフィット
Kubernetes	Amazon Elastic Kubernetes Service (EKS)	セキュリティコンプライアンスとモニタリングを自動化して、コンテナ、Kubernetes、クラウドを安心して稼働させます。
クラウドコンテナ	AWS Elastic Container Service (ECS)	コンテナ、Kubernetes、クラウドを自信を持って実行するために、セキュリティコンプライアンスとモニタリングを自動化します。

セキュリティ

セキュリティレイヤー	AWSソリューション	Sysdig+AWSのベネフィット
ホストOS	Amazon Linux 2, Bottlerocket	基盤となるEC2ホストの構成を継続的にスキャンし、CISのベンチマークに適合していることを確認する。
アクセスコントロール	AWS Identity and Access Management (IAM)	IAMの変更を監視し、予期せぬ変更やセキュリティ上の脅威がないかを確認する。 サービスベースのアクセスコントロールを導入して、セキュリティと監視情報を個々のユーザー／チームに効率化する。
イメージスキャンと脆弱性管理	ClairによるAmazon ECRのスキャン（パッケージイメージのスキャン）	CI/CDパイプラインやレジストリ（ECR、CloudBuild、CloudPipeline、Quay、DockerHubなど）内のデプロイメント前のイメージをスキャン。 ランタイムの脆弱性レポートを取得し、新しいCVEの影響を評価することができます。
コンプライアンス	AWS Config	CIS、PCI、NIST、SOC 2などに対応したすぐにできる構成チェックで継続的なコンプライアンスを実施し、カスタム評価やダッシュボードで報告する。
ネットワークセキュリティ	Amazon EC2 security groups	ネイティブのKubernetesネットワークポリシーの使用を自動化、簡素化。 ポッド、サービス、アプリケーション間のすべてのネットワーク通信を可視化。あらゆるプロセスとの接続を監査し、コンテナセキュリティにゼロトラストアプローチを導入します。

ファイル整合性監視		Sysdig Secureファイルシステムポリシーにより、ファイル整合性監視（FIM）を迅速に実装し、ファイルやディレクトリへの不審な変更を警告することが容易になります。
クラウドワークロード保護 ランタイム検知と脅威の防止		任意のAWS、ECS、EKSのラベル／メタデータに基づいてランタイムセキュリティポリシーを適用し、異常な動作を検知・防止します。 システムコール、CloudTrailログ、監査イベントを通じた深い可視性とAWSメタデータを組み合わせて、攻撃を検知し、ブロックします。オープンソースのCNCFランタイムセキュリティプロジェクトであるFalcoを搭載。
クラウドセキュリティポスチャー管理	AWS CloudTrail CIS AWS Foundation Benchmarks AWS GuardDuty	クラウドアセットをディスカバーし、構成上の問題を可視化し、クラウドサービスに対する脅威を検出します。Sysdigは、CSPMとクラウド脅威の検知をクラウドワークロード保護と統合し、AWSクラウドサービスの脅威を検知する時間を短縮します。
コンテナフォレンジック		ECSやEKSがコンテナ/ポッドを終了させた後でも、フォレンジックや事後分析を行うことができます。

まとめ

AWSのクラウドとコンテナサービスは、企業が顧客や市場のニーズを満たすソリューションを提供するための迅速な行動と革新を支援しています。AWSは、クラウドアカウント、ワークロード、コンテナのセキュリティと監視をカバーしています。Sysdigは、アプリケーション、クラスター、拠点、統合を拡大する際に、オープンソースイノベーションに基づいて構築されたコンテナとクラウドのセキュリティスタックにより、コンテナ、Kubernetes、クラウドを自信を持って実行できるようにします。Sysdigは、深く統合されたセキュリティと可視性でAWSサービスを補完します。また、AWSのパブリッククラウドとハイブリッドクラウドのインフラストラクチャーを使用して、どこでもワークロードを保護し、実行と拡張が非常に容易に行えるようにします。

追加リソース

パートナーシップ概要

- Sysdig/AWSパートナーシップページ
- Sysdig/AWSパートナーブリーフ

顧客事例：

- Pike13、Amazon ECS上でアプリケーションのアップタイムを最大化し、より高い効率性を実現
- JW Player、AWS上での驚くべき動画体験を1B以上のユーザーに提供
- Worldpayは、PCI準拠のペイメントソリューションを迅速に提供することで、競争力を高めます
- 株式会社エヌ・ティ・ティ・データ デジタルペイメント開発におけるコンテナとSysdigの活用紹介

Webinar：

- Accelerate Threat Detection Across AWS Cloud and Containers
- Ship Apps Faster on AWS with Unified Visibility and Security

Sysdig Secure DevOps Platformが、お客様とお客様のチームが本番環境でクラウドネイティブアプリケーションを自信を持って実行できるようにする方法をご紹介します。

プラットフォームの詳細についてはお問い合わせください。

---

sysdig.jp