AWSクラウドとコンテナのための継続的なセキュリティ

sysdig

目次

AWSクラウドとコンテナのための継続的なセキュリティ

現代の企業や組織が活動する上で、ITリーダーにとってスピードやアジリティ（俊敏性）、スケーラビリティは、今や、中核となるものに変化してきました。CIOにとって、迅速な行動とイノベーションを可能にする最新の基盤を確保することは必須の課題となっています。

このような要求を満たすには、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、コンテナベースのアプリケーション開発とDevOpsアプローチにより、開発チームはソフトウェアを迅速にスピンアップし、調整を行い、顧客と市場のニーズを満たすソリューションを継続的に提供できるようになります。

このような変化は、単にビジネスのやり方をデジタル化しただけのものではなく、クラウドやコンテナといった基本的な部分が、まったく新しいビジネスのあり方を可能にしているのです。

上述の内容を実現するには、クラウドとコンテナが持つスピードとアジリティに追随しつつ、より迅速な成果をもたらすために、プロセスを減速させないような補完的なセキュリティが必要です。このように、クラウドとコンテナのセキュリティを確保しながらデリバリーを加速するという二重の目標があるため、データとワークロードの保護と、アジャイルなアプリケーション開発の促進を両立させるアプローチが必要になるのです。言い換えれば、安全を確保しつつ、スピードを落とさないということです。

一方、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では、これまでのセキュリティ対策はうまく機能しません。コンテナは可搬性と隔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すのに最適ですが、企業が最初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プロセスの確立や、コンテナの安全性と信頼性の高い運用という課題に直面することになります。クラウドにワークロードを展開する場合、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ーとして機能し、数分または数秒ごとに変化することで常に変化するセキュリティ環境を作り出してしまいます。このような新しいソリューションの利用は、ビジネスの迅速な動きを可能にしますが、その一方で、新たな潜在的脅威をもたらすことにもなります。

Amazon ECS、Amazon EKS、AWS FargateなどのAmazon Web Services（AWS)のクラウドとコンテナサービスを採用して、大規模なアプリケーションを迅速に提供するクラウドチームが増えてきています。コンテナとオーケストレーションによるアーキテクチャーのロールアウトに伴い、アプリケーションと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るのです。

Sysdig Secure DevOps Platformは、コンテナ、Kubernetes、そしてクラウドの安全な実行を可能にするセキュリティを提供します。Sysdigを利用することで、ビルドの保護、脅威の検知と対応、クラウドの体制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、当社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を監視し、トラブルシューティングを行うことで、パフォーマンスと可用性の最大化を支援します。Sysdigでは、ランタイム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。

Sysdigを通じて、セキュリティ、コンプライアンス、監視を統合したセキュアなDevOpsワークフローを構築することで、導入を加速でき、AWS上の本番環境で自信を持ってコンテナとクラウドのワークロードを実行できるようになります。これにより、次のことが可能になります。

- ビルドプロセス中にセキュリティポリシーと構成を検証することで、導入をスピードアップすること
- クラウドのセキュリティ体制とコンプライアンスを継続的に評価すること
- パフォーマンスに影響を与えずにランタイムの脅威を阻止すること
- 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健全性を監視することで、問題を未然に防ぐこと
- 詳細な記録を使用してインシデント対応を実施すること

このガイドでは、AWS環境の包括的なクラウドとコンテナセキュリティを確立するためのフレームワークを紹介するほか、SysdigがAWSのネイティブツールをどのように補完し、強化できるかについて具体的な推奨事項を紹介します。

AWS利用者にとって、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、クラウドインフラストラクチャーの保護に重要な3つの要素があります。

責任共有によりセキュリティを実現

AWSのようなパブリッククラウドにおいて、セキュリティはユーザーとの共有責任となります。AWSは環境のセキュリティを処理し、利用者は環境内で発生するすべてのことに責任を負います。AWSは、ユーザー認証、Amazon Simple Storage Service（S3）バケットの監視、AWS CloudTrailによるロギングと監視など、すぐに使えるセキュリティ機能を提供しています。しかし、利用者は、ワークロード全体の設定ミス、既知の脆弱性、および動作の異常をどのように特定して修正するかについても考慮する必要があります。

クラウドの継続的な変更には、継続的な監視が必要です。このような監視は、クラウドとオーケストレーションのすべての活動において機能し、使用中のクラウド資産と監査設定の可視性を提供する必要があります。また、クラウドとコンテナのアクティビティを継続的にスキャンして分析することで、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。

自動化による移行の高速化とセキュアなスケーリング

セキュリティチームとDevOpsチームは、セキュリティ制御が実際に意図したとおりに機能しているか、またそれが開発作業を遅らせていないかを検証する必要があります。多くの企業は手動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、これを効果的に行う唯一の方法です。そのため、企業は、手動プロセスなしでクラウドのアクティビティを分析し、最大規模の環境でも期待どおりに動作しているかどうかを把握できるようなツールを必要としています。

自動化されたアプローチにより、クラウド上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を出すことが可能となります。これにより、脆弱性や問題が悪用されることで、開発プロセスのスピード低下や、ビジネスアプリケーションに影響が出る前に対処できるようになります。

開発とコンテナオーケストレーションの最適化

AWSは、Amazon Elastic Kubernetes Service（EKS）とElastic Container Service（ECS）という2つのコンテナサービスを提供しています。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。そして、コンテナ化されたワークロードのセキュアな作成とデプロイをサポートするような開発と運用、セキュリティの各プロセスを最適化します。さらにコンテナアプリケーションのデプロイを加速するように設計されています。ECSとEKSと共に、利用者は、コンテナ用のサーバーレスコンピュートエンジンであるAWS Fargateも利用できます。

このようなオーケストレーション化されたアプリケーション環境では、従来のセキュリティツールはもはや機能しません。なぜなら、従来のセキュリティツールは、コンテナの内部を見ることができず、Kubernetesの動的な性質にも対応できず、クラスター、アベイラビリティゾーン、およびリージョン間でのスケーリングが行えないからです。必要となるのは、コンテナ、Kubernetes、クラウド向けに構築され、DevOpsワークフローに統合された、コンテナおよびクラウド用のセキュリティスタックです。

さまざまなAWSユーザー固有のニーズに対応

組織内のチームや役割によって、可視性やセキュリティに対する懸念や視点は異なり、また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も異なります。

開発者

AWSは、開発者がインフラストラクチャー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活用できるように、開発者を支援します。AWSのCI/CD（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結合するためのAWS CodeBuildやAWS CodePipelineなどのAWSフレームワークを使用すると、開発者はGitHubなどのリポジトリに変更をプッシュできます。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それをプッシュします。コンテナイメージに既知の脆弱性がなく、イメージが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保証することは大きな課題ですが、それはしばしばアプリケーションの整合性を損ない、リリーススケジュールを遅らせる可能性があります。

クラウド/DevOps

クラウドおよび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の維持に責任を負っています。ユーザーは、組み込み型のAWS Webコンソールを活用することで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できるほか、プレイブックを利用することでアプリケーションの導入を自動化できます。DevOpsチームには、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セキュリティポリシー、ネットワークポリシーなどの機能を利用して、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ています。

セキュリティとコンプライアンス

セキュリティ運用、SecOps、DevSecOps、CSIRTの各チームは、クラウドの責任共有モデルに従って行動します。しかし、脅威の防止、リスクの特定、脆弱性の切り分けを効果的に行うためには、セキュリティチームがAWSクラウドやコンテナ環境を継続的に監視して異常な動作やゼロデイ攻撃から保護し、違反が発生した場合にはインシデント対応を実施しなければなりません。また、セキュリティチームは、コンプライアンスの枠組みや社内要件に基づいてポリシーを設定し、そのポリシーを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ーやアプリケーションを特定し、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かどうかを監視する必要があります。

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

セキュリティ、コンプライアンス、監視を統合することで、プライベートクラウド、ハイブリッドクラウド、マルチクラウドの各環境において、AWSコンテナサービス上でクラウドネイティブなワークロードの構築と実行を確信を持って行えるようになります。これらの重要な機能を自動化してセキュアな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他のデータリポジトリ間で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リリースを実現できるようになります。

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、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に必要な基本的なカバレッジを提供します。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することで、追加のセキュリティと監視機能を提供します。これにより次のことが可能となります。

- ビルドパイプラインの保護
  - CI/CDパイプラインとレジストリ内のスキャンの自動化
  - コンテナとホストのスキャンを統合
  - 効率的に脆弱性にフラグを立て、オーナーを特定すること
  - 脆弱性のあるイメージの導入をブロックすること
- 実行時の脅威を検知して対応すること
  - 脅威検知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、ゼロデイ脅威の検知を実装すること
  - 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すること
  - 詳細な記録を使用してインシデント対応を実施すること
  - Fargate、ECS、EKSなどのクラウドとコンテナサービスに対するランタイムの深い可視性を確保すること
- クラウドの体制とコンプライアンスを継続的に管理すること
  - ビルド時と実行時に設定ミスやコンプライアンス違反を特定すること
  - 個人やグループレベルでのアカウントとアクセスのセキュリティを監視すること
  - 詳細なレポートによる進捗の確認をすること
  - PCI、NIST、SOC2に対応した「すぐに使える」ポリシーで時間を節約すること
- コンテナ、Kubernetes、クラウドサービスを監視すること
  - パフォーマンスとキャパシティを監視することで、問題を未然に防ぐこと
  - きめ細かいデータを使用してトラブルシューティングを高速化すること
  - 複数のクラスターやクラウドにまたがるPrometheusの監視をスケーリングすること
  - コンテナアクティビティを監査し、インシデント対応を迅速化すること

Sysdigでは、クラウドとコンテナのセキュリティと監視機能を備えた、唯一の包括的な統合プラットフォームを提供しています。このプラットフォームは、クラウドワークロード保護プラットフォーム

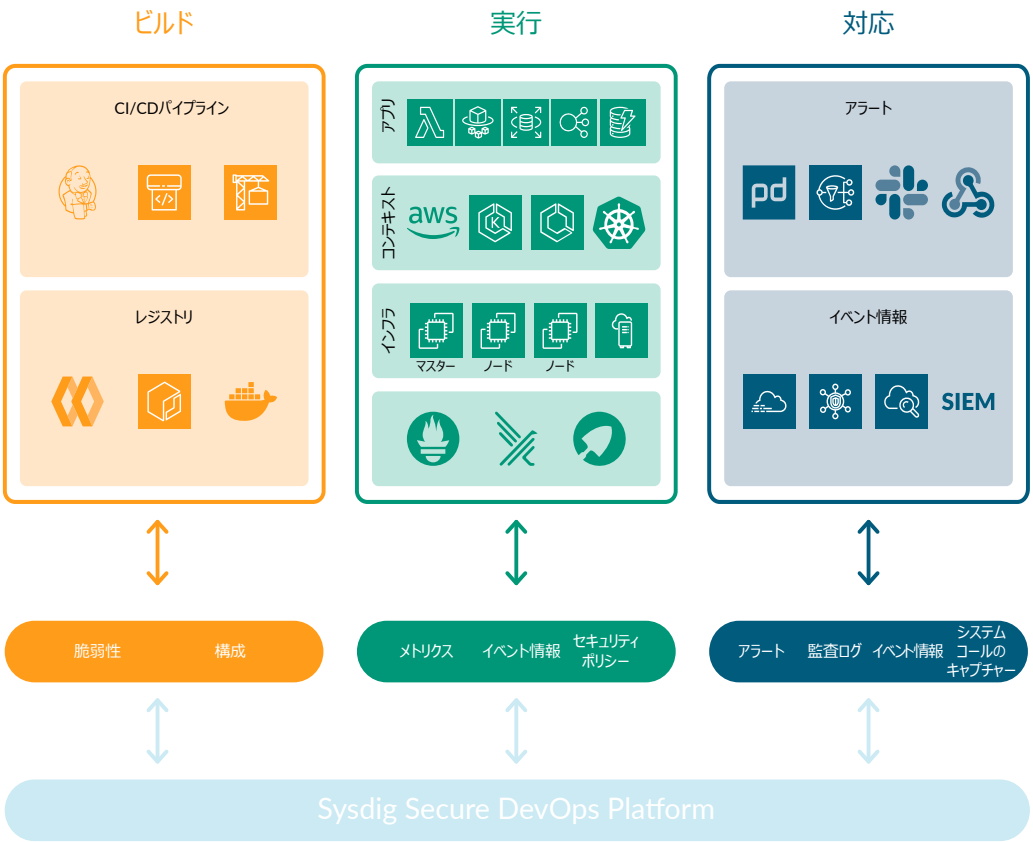
（CWPP）とクラウドセキュリティポスチャー管理（CSPM）の機能、および健全性とパフォーマンスの監視機能を組み込んでおり、クラウドワークロード、アカウント、コンテナ、Kubernetesを通じた1つの「信頼できる唯一の情報源」をDevOpsチームとセキュリティチームに提供します。

これらのツールは、AWS環境上で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、およびセキュリティチーム間に存在する情報のサイロ化を排除します。Sysdigを使うことで、セキュリティチームとDevOpsチームは、インシデントの正確な特定とトリアージ、原因の迅速な特定が行えるほか、既に終了して稼働していないコンテナワークロードに関するフォレンジックをも実施できるようになります。

Sysdigプラットフォームを使用することで、セキュリティチームとDevOpsチームは、疑わしいユーザーの行動、データへの脅威、特定のネームスペースやクラスターで実行中の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できます。たとえば、新しい脆弱性が報告された場合、Sysdigを使うことで、DevOpsチームは、特定のパブリッククラウド（AWS）リージョン、ネームスペース、クラスターなどにおいて影響を受けるイメージと、修正を所有するチームを迅速に特定できるようになります。このアプローチを通じて、クラウドとKubernetesの両方のコンテキストに自動的に相互関連付けされた脆弱性と、きめ細かいシステムデータを分析することで、問題を迅速に解決できるようになります。

当社では、信頼できる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一元的な可視化とセキュリティを提供しています。Sysdigは、AWSでホスティングされるSaaSファースト型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展開することで、Sysdigプラットフォームは10,000以上のノードにスケーリングすることが可能であり、AWSコンテナサービスクラスター上で動作するコンテナとアプリケーションの保護と監視を実現します。

ガイド付きのオンボーディング、すぐに使えるダッシュボード、厳選されたワークフローを通じて、簡単に利用を開始できます。Sysdigは、自動化とすぐに使える統合機能により、クラウド環境と既存のDevOpsワークフローへの統合を実現するため、可視性やセキュリティ管理の速度が低下することはありません。



Sysdigは、AWSのコンテナサービスに関するコンテナやオーケストレーションのインサイトを、次の機能を使用して提供します。

- ImageVision™は、脆弱性や設定ミスのあるイメージを特定し、そのようなイメージがデプロイされるのを防止します。
- ContainerVision™は、コンテナ内やマイクロサービス全体のリクエストレベルの可視性を提供します。これは、侵襲的なインストルメンテーションを行うことなく、詳細なメトリクスとイベントを提供します。
- ServiceVision™は、ECSおよびEKSと統合して、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のメタデータにより自動的にリッチ化します。
- 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保護

このセクションでは、AWSが提供する各種のセキュリティコントロールを紹介するほか、Sysdigがクラウドネイティブスタックとコンテナライフサイクルにわたってソリューションのセキュリティ、コンプライアンス、監視をいかに拡張するかを紹介します。

AWSは、次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を含むセキュアなホスティングインフラストラクチャー
- AWS Identity and Access Management (IAM) によるアクセス制御
- 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実施

ホストのセキュリティ

クラウドセキュリティは、AWSの最優先事項です。AWS利用者はセキュリティに最も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ーの恩恵を受けることができます。マネージドサービスであるAmazon EC2は、AWSのグローバルな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、EC2インスタンスに対してホストベースの制御を含む階層型アプローチをを推奨しており、これにより環境へのアクセスを制限できます。一般的に、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）を採用しています。Amazon CloudWatchは、HIDSから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が提供する機能

AWS上でコンテナをセキュアに運用するために、Amazon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セキュアで安定した高性能のオペレーティングシステムを提供しています。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。これは、重要でないパッケージの数を減らすことで、潜在的なセキュリティの脆弱性にさらされる機会を制限しています。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、Linuxベースのオープンソースosであり、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が専用に構築したものです。Bottlerocketには、コンテナを実行するために不可欠なソフトウェアのみが含まれており、リソース使用率の向上、セキュリティ上のアタックサーフェスの縮小、管理オーバーヘッドの低減を実現しています。Bottlerocketでは、セキュリティアップデートを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可能であり、障害が発生した場合はロールバックを実行できます。

これらのソリューションは、クラウド上でのセキュアな運用を可能にするだけでなく、AWS Outpostsを利用してオンプレミス施設でも活用することが可能です。Sysdigは、パブリック、プライベート、およびハイブリッド環境において、Amazon Linux 2とBottlerocketの両方でセキュリティ、監視、コンプライアンス機能を検証しています。これにより、これらのソリューションとAmazon EKSおよびECSを使用して、セキュアにかつ一貫して本番環境でコンテナワークロードを実行できることが保証されます。

Sysdigが追加する機能

Sysdigはホストスキャンを提供することで、仮想および物理サーバーまたはクラウドネイティブホストインスタンス上のパッケージの脆弱性を検知できるようにします。詳細なレポートにより、運用チームは、侵入やゼロデイ脆弱性攻撃などのインシデントを回避するために何にパッチを適用すべきかを把握できます。

Sysdig Secureは、ホストOSと非OSパッケージの検知機能を提供し、クラウドとKubernetesの豊富なコンテキストを使用して影響と所有権を評価することにより、修正に要する時間を短縮します。また、ホストとコンテナに対応した単一の脆弱性管理ソリューションにより、リスクを低減し、規制要件とコンプライアンスに対応できるほか、ワークフローの統合により時間を節約できます。

ユーザー認証と権利認証

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、相互作用する能力を提供します。これにより、企業が個人とグループに許可を与えることが可能となります。管理者は、一元化されたソースを通じて、役割、組織、地域、またはワークロードと他のリソースのセキュリティの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できます。

ユーザーはAWSのクレデンシャルに基づくリクエストを通じて、各種のサービスにアクセスします。しかし、S3ストレージのようないくつかのリソースについては、そのソースのみにユニークなアクセスを提供するために、きめ細かなレベルの許可を付与できます。リクエストのコンテキストは、AWSユーザーが自分の環境に適用してい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、パーミッションのための事実上のソースとして動作します。

AWSサービスへの特定のアクセスは、Web UI、CLI、およびAPIを含む標準的なインターフェイスを介して提供されます。さらに、AWSサービスはAWSコンテナサービスと相互作用することで、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できるようになります。CI/CDパイプラインが新しい導入を本番環境にプッシュすることを想像してください。誰が何をできるかを、いかにして制御して測定するのでしょうか？

AWSが提供する機能

AWS IAMを使用すると、AWSサービスやリソースへのアクセスを安全に管理できます。IAMを使用すると、AWSユーザーとグループを作成して管理し、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できるようになります。IAMの管理者は、EKS、ECS、Fargateのリソースを使用するためのユーザー認証（サインインが可能であること）と権利認証（パーミッションを持つこと）を受けることができる人を制御します。

Sysdigが追加する機能

Sysdigを使用すると、お使いのAWSコンテナサービスに関する可視性、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ユーザーのグループを定義できます。これはSysdig Teamsと呼ばれるものであり、既存のAWS IAMメカニズムを補完するために、サービスおよびメタデータベースのアクセス制御の概念を導入しています。

Sysdig Teamsを利用することで、管理者はAWS上に展開された特定のサービスや限定されたサービス群にアクセスできるユーザーグループを定義できます。たとえば、アプリケーションのオーナーは、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。また、アクセス制御で露出を制限し、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、ユーザーとチームのセキュリティ情報を効率化できます。

Sysdigは、ユーザー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制御を実現します。管理者ロールに加え、表示のみ、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利用できます。

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ストラクチャーのコンポーネントは、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のソフトウェアであり、古いバージョンのライブラリ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元々どこから来たのか、誰が作ったのか、そしてパッケージ内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が提供する機能

Amazon Elastic Container Registry (ECR) は、開発者がDockerコンテナイメージを簡単に保存、管理、導入できるようにするフルマネージド型のDockerコンテナレジストリです。ECRは、ECSやEKSといったAWSのコンテナサービスと統合されており、これを使うことで開発から本番環境までのワークフローを簡素化できます。

ユーザーがAWS上のコンテナの採用を開始する場合、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になります。ECRは、オープンソースのClairプロジェクトの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。ユーザーは、ECRから取得したイメージをスキャンして、脆弱性と設定ミスの両方がないことを保証する必要があります。これにより、AWS上で動作しているアプリケーションのうち悪用されているものをプッシュすることを防止できます。

Sysdigが追加する機能

Sysdig Secureは、Kubernetesのライフサイクルのすべての段階において、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することで、Sysdig Secureは、脆弱性、セキュリティ、コンプライアンス関連の設定ミスを検知するための単一のワークフローを提供します。お客様のチームがアプリケーションを構築する際、SysdigはCI/CDパイプラインを通じて脆弱なイメージがプッシュされるのを防ぎ、本番環境における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を越えて拡張された、追加のECRスキャン機能を提供します。ECRが設定されている場合、Sysdig Secureはレジストリ内に保存されているイメージを解析のためにエンジンに取り込みます。導入前に脆弱性、コンプライアンスチェック、設定ミスをスキャンできます。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、Java JARファイルなどのサードパーティライブラリから検知できます。これらは、本番環境に移行する前に、開発者がアプリケーションイメージに取り込むことができます。

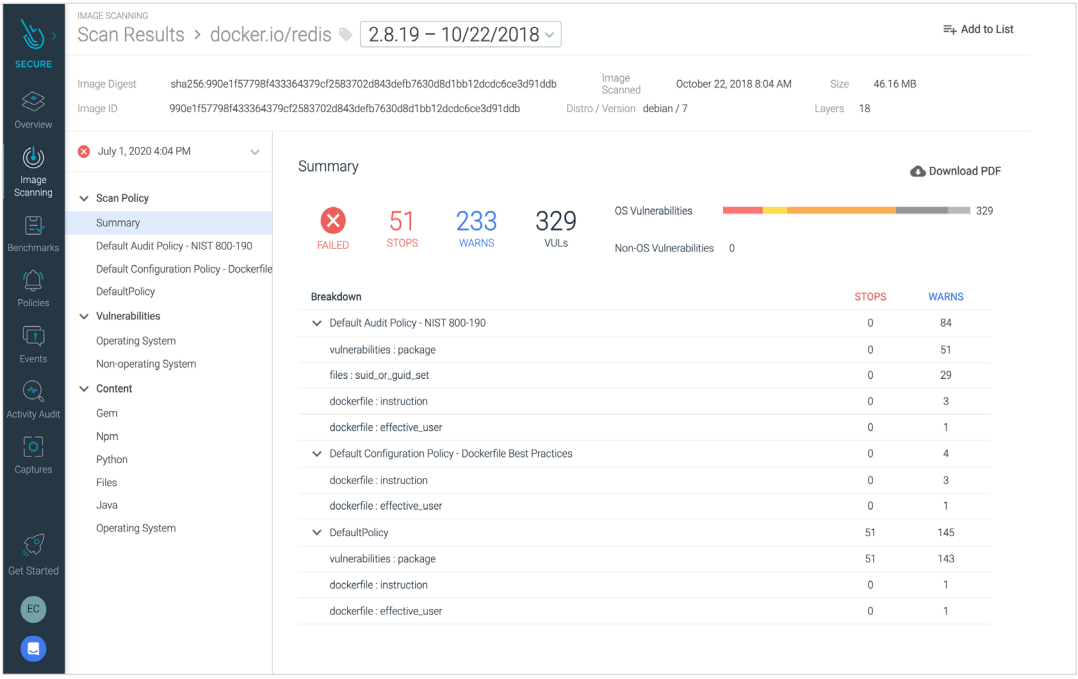
導入前のスキャンに関しては、Sysdigは2つのコンテナイメージスキャンオプションを提供しています。

- Sysdigにイメージを送信してスキャンするようユーザーに求める標準的な方法です。スキャン後、ユーザーはSysdig Secure UIで結果を確認できます。
- ローカルスキャンは、インラインスキャンとも呼ばれ、CI/CDパイプラインまたはECRレジストリ内で直接イメージをスキャンするものです。このオプションは、レジストリの認証情報やイメージのコンテンツをAWS環境の外部と共有する必要がないため、よりセキュアなアプローチを可能にします。また、スキャンが自動化され、ECR内で直接レポートが生成されるため、スキャン結果を迅速に得ることができます。

Sysdig Secureは、次のものに関する可視性を提供します。

- OS公式パッケージの脆弱性
- 非公式パッケージの脆弱性
- 設定のチェック（DockerfileでSSHポートがオープンされている、rootとして実行可能なユーザー設定など）
- JavascriptのNPMモジュール、PythonのPiP、RubyのGEM、JavaのJARアーカイブなど、サードパーティライブラリにおける脆弱性
- Secret情報、、クレデンシャル（トークンや証明書など）、およびその他の機密データ
- 既知の脆弱性と利用可能なアップデート
- 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に対するコンプライアンスチェック

これらのアーティファクトは、特定のレジストリ、リポジトリ、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保存評価されます。Sysdig Secureのスキャンポリシーを使うと、イメージ内にある脆弱性、設定ミス、コンプライアンスの問題を検知した上で、UIを通じて直接合格/不合格の結果を生成できるようになります。



Fargateイメージのローカルスキャン

FargateのユーザーにとってのSysdigソリューションのユニークな機能として、Fargateタスクの開始と同時にECR内のイメージのスキャンをトリガーできることが挙げられます。Amazon EventBridgeを活用することで、SysdigはFargateのリクエストをインターセプトし、イメージを識別し、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により、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保証できます。

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、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、顧客により速く、より頻繁にアップデートを提供できるようにするものです。アプリケーションを構築する際にセキュリティをデリバリーパイプラインに組み込むことで、脆弱性の特定と対処を迅速化し、開発者の生産性を維持できます。

AWSが提供する機能

AWSでは、CI/CDパイプラインを設定することで、ソフトウェアデリバリープロセスを自動化できます。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、コードのビルドとテストのためのCodeBuild、そしてコードの自動導入のためのCodeDeployです。CodePipelineは、これらのすべてのツールの上位に立つことで、これらのツールが各種の段階を可視化し自動化できるようにします。

AWS CodeBuildは、ソースコードをコンパイルし、テストを実行し、導入可能なソフトウェアパッケージを生成する、フルマネージド型のCI（継続的インテグレーション）サービスです。CodeBuildは継続的にスケーリングを行い、複数のビルドを同時に処理するため、ビルドがキュー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、フルマネージド型のCD（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、コードの変更があるたびに、リリースプロセスのビルド、テスト、導入の各フェーズを自動化します。

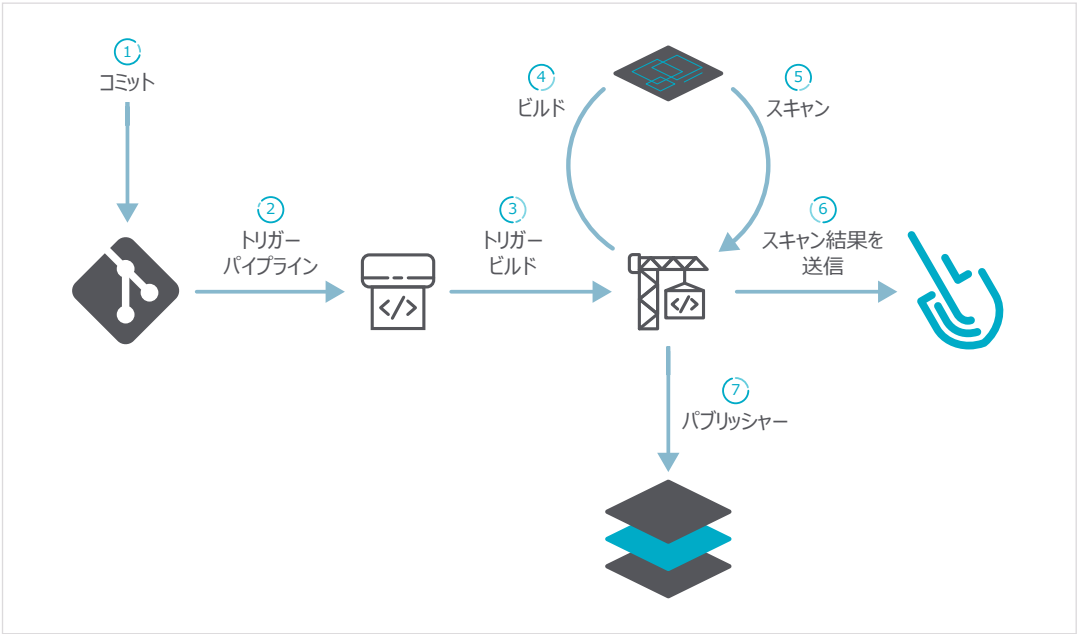
Sysdigが追加する機能

AWSで使用されるCI/CDパイプラインのためのイメージスキャンは、パイプラインの早い段階で既知の脆弱性を検知し、コンテナビルド構成を検証することで、導入のセキュリティに対するDevOpsチームの信頼性を高めます。コンテナレジストリへのイメージの公開や本番環境への導入前にこれらの問題を検知することで、修正を迅速に適用し、本番環境への移行時間を短縮できます。

Sysdig Secureのイメージスキャンは、AWS CodeBuild、AWS CodePipeline、Jenkins、Bamboo、GitLab、CircleCI、Tektonなど、選択したCI/CDパイプラインに直接統合できます。これにより、サードパーティライブラリ、公式/非公式OSまたはパッケージ、設定チェック、クレデンシャルの公開、メタデータの脆弱性や設定ミスを検知できます。また、Sysdigのローカルインラインスキャンを使用すると、イメージがレジストリにプッシュされる前に問題を検知できます。

SysdigのスキャンとCI/CDパイプラインの統合により、開発者はCI/CDツール内で直接必要な情報を入手し、スキャンが失敗した理由と修正すべき点を理解できるようになります。重要でないポリシー違反については、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る必要があるかを警告で示します。

Sysdigを利用することで、AWS CodePipelineで構築したイメージをインフラストラクチャーの外部に出すことなくスキャンできるようになるため、ステージングレジストリが不要になります。されに、複数のスキャンを並行して実行することで、スループットを向上できます。



イメージ保証

イメージ保証は、未承認のイメージがコンテナ環境に導入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および検証することで、問題やエラーを減らすことができます。

AWSが提供する機能

KubernetesアドミッションコントローラーをEKSと組み合わせて使用することで、承認されていないイメージがオーケストレーションされたコンテナクラスターに導入されるのを防ぐことができます。EKSは、このKubernetes機能を利用して、Kubernetes APIへのリクエストの評価をサポートすることにより、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できるようになります。

Sysdigが追加する機能

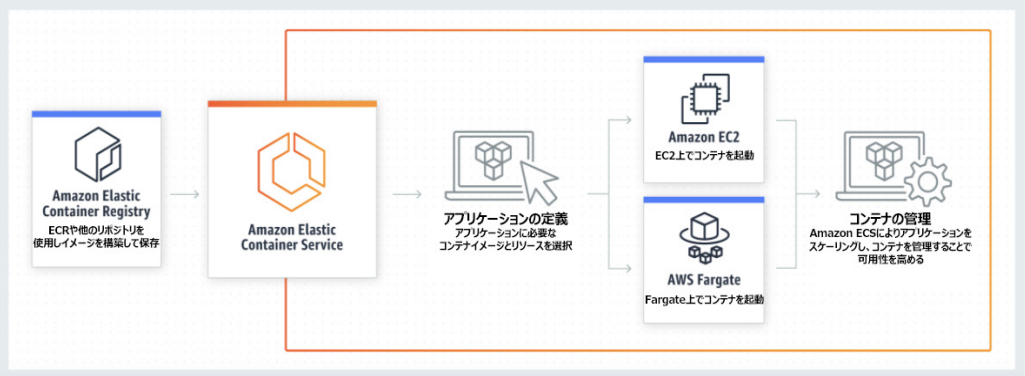
EKSは、Sysdig Secureと照合して、イメージが設定されたセキュリティポリシーに準拠しているかどうかを評価できます。アドミッションコントローラーを使用する場合、このセキュリティ検証の決定がAPIに伝搬されます。APIはオリジナルの要求者に返信した後、イメージがチェックに合格した場合のみ、オブジェクトをetcdデータベース内で永続化します。

レジストリのセキュリティ

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となります。RBACを使用して、誰がコンテナイメージのプルおよびプッシュを行えるかを管理することや、プライベートレジストリを使用することは、組織を保護するために取ることができる手順の一部です。

AWSが提供する機能

Amazon ECRは、高い安全性、拡張性、信頼性を備えたマネージド型の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通じてプライベートDockerリポジトリをサポートし、特定のユーザーまたは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るようにします。開発者は、Docker CLIを使用して、イメージのプッシュ、プル、および管理を行うことができます。



Sysdigが追加する機能

Sysdig Secureのコンテナイメージスキャンは、Docker v2対応のレジストリすべてをサポートしています。これには、CoreOS Quay、Amazon ECR、DockerHub Private Registries、Google Container Registry、Google Cloud Artifact Registry、JFrog Artifactory、Microsoft ACR、SUSE Portus、VMware Harborなどが含まれます。

コンプライアンス

AWS上でマイクロサービスを実行するエンタープライズコンピューティング環境は、相互接続された数百または数千のアプリケーションとサービス、および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制御し続けるには、セキュリティポリシーに準拠してシステムをスキャンするための標準的な方法が必要です。

AWSが提供する機能

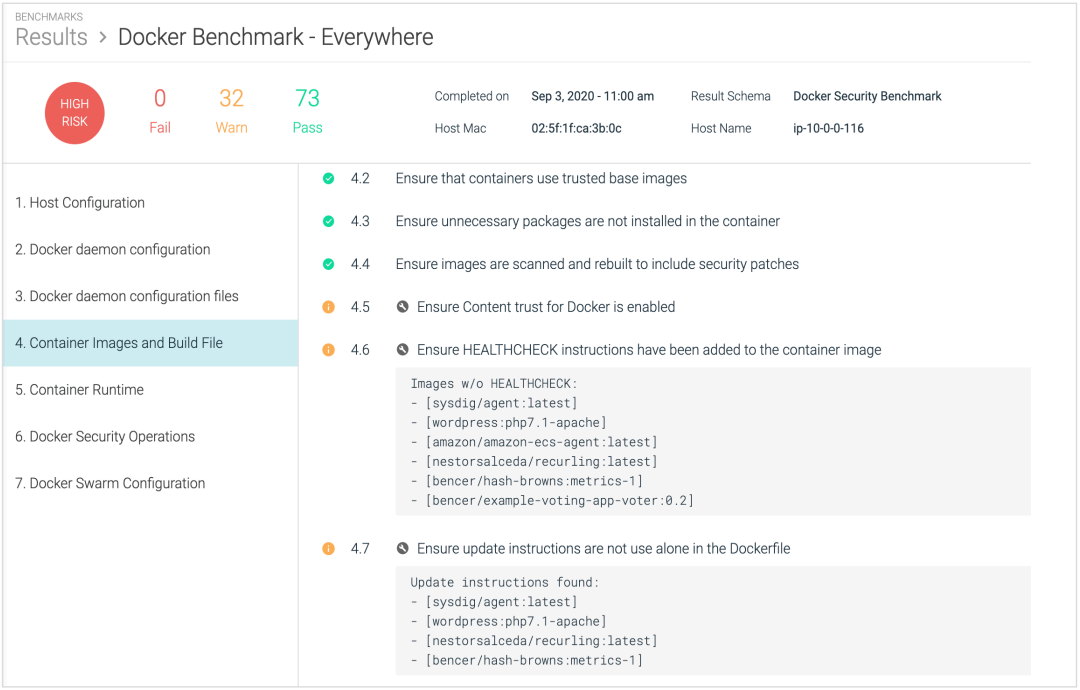
AWS Configは、AWSリソースの構成の評価、監査、および査定を可能にするサービスです。これにより、AWSリソースのサービス構成を継続的に監視、記録し、記録された構成と望ましい構成との評価を自動化できます。また、これにより、コンプライアンス監査、セキュリティ分析、変更管理、および運用上のトラブルシューティングを簡素化できます。

Sysdigが追加する機能

Sysdigは、NISTやPCIなどの標準に対応したコンテナライフサイクル全体のコンプライアンスを拡張します。導入が望ましい設定に準拠していることを検証できることは、コンプライアンスを実現するための最初のステップです。しかし、コンプライアンス要件はこれで終わりではありません。コンテナに対するコンプライアンスには独自の要件があり、さまざまなポイントで実施する必要があります。これには次のものが含まれます。

- AWS、Docker、KubernetesのCIS（Center for Internet Security）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ベストプラクティスに照らし合わせてチェックすること。
- ビルド時に、コンテナイメージのスキャンポリシーをNIST 800-190、PCI、HIPAAなどの標準に対応させること。
- 実行時には、MITRE ATT&CKのような攻撃フレームワークを継続的に検知するためのポリシーや、導入後のコンプライアンスをチェックするためのポリシーを使用すること。
- コンテナ環境におけるあらゆる変更を監査すること（これは、SOC2、PCI、ISO、HIPAAの各要件に含まれています）。

Sysdigでは、コンプライアンスダッシュボードを使用して進捗を確認できます。インフラストラクチャー層から始まり、Sysdigは、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、特定のホスト、プラットフォーム、コンテナに関するコンプライアンスチェックを実行します。また、Sysdigは、ポリシー違反を修正するためのガイダンスを提供します。これにより、設定上の問題が発生した場合、より迅速に問題を解決できるようになります。

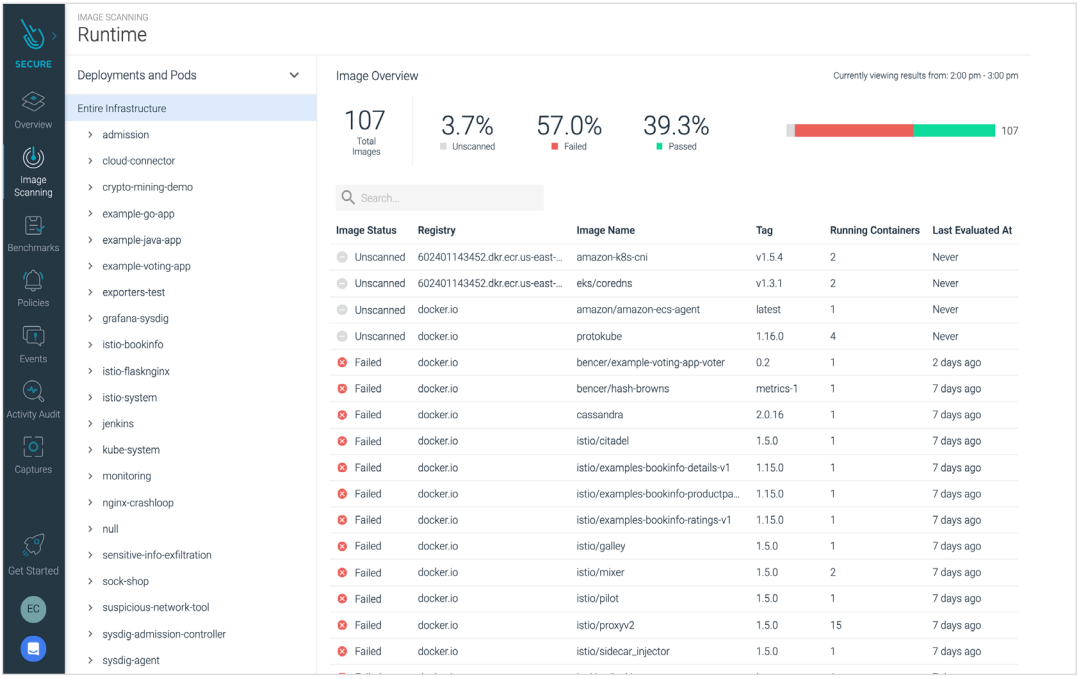


Sysdig Secureは、コンテナイメージのセキュリティと、NIST SP 800-190、PCI DSS、Dockerfileなどのコンプライアンスのベストプラクティスを実装するためのツールを提供します。Sysdig Secureのコンテナイメージスキャンポリシーを使用することで、クラウドのコンプライアンスを検証し、次のようなベストプラクティスをイメージレベルで実施できます。

- 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
- コンテナには信頼できるベースイメージを使用し、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、または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に変換することで、実行時のコンプライアンス保証を提供します。また、Sysdigは、導入後のコンテナの挙動を分析し、実行時のドリフトを監査します。さらに、Sysdigは、システム上で実行されるあらゆるコマンド（docker execやoc attachなど、ホスト上および任意のコンテナ内部の両方で実行されるもの）を利用するか、またはKubernetes APIを利用することで、目的とする監査（Secretリソースへのアクセスや、未承認ユーザーによるリクエストなどの監査）を実現します。

新たな高リスク/クリティカルなCVEが公開された場合、、直ちに自らが「どの程度リスクにさらされているか」を評価できます。続いて、影響を受けるサービスや責任を負う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オーナーは、サービス、導入、アプリケーションなどのKubernetesまたはクラウドのメタデータを使用して特定され、イメージと脆弱性を表示するためにアラートが送信されます。



ネットワークセキュリティ

アプリケーションのコンテナやクラウドへの移行は、セキュリティモデルを見直すきっかけとなります。多くのクラウドチームは、組織内部のネットワークに対しても、ユーザー認証と権利認証を要求するゼロトラストアプローチを採用しています。

ネットワークをセグメント化、隔離、制御する機能は、ゼロトラストにとって重要な制御ポイントであり、コンテナやKubernetes環境において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なものとなっています。

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のに苦労するようになり、オープンネットワークポリシーを利用した悪意ある試みを見逃す可能性があります。Kubernetesでゼロトラストネットワークセキュリティモデルを適用するには、アプリケーションがどのように使用されているかを知らなければ困難です。

AWSが提供する機能

AWS上のコンテナ型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クラスターで実行中のPod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。

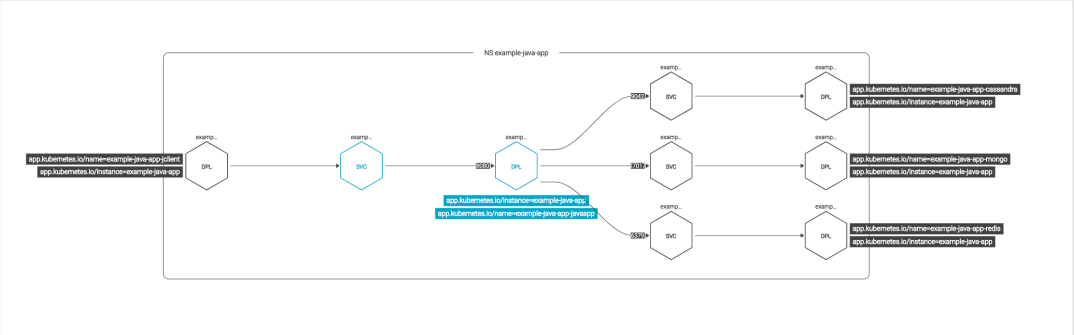
Pod向けのセキュリティグループは、ネットワークセキュリティの要件が異なるアプリケーションを共有のコンピュート資源上で実行することで、ネットワークセキュリティのコンプライアンスを実現します。

ネットワークセキュリティのルールはEC2セキュリティグループ内で定義し、KubernetesネイティブAPIを使用するアプリケーションのPod間およびPodと外部の間でのAWSサービス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を通じて運用に関する知識とツールを再利用することにより、ネットワークレイヤーと認証レイヤーでセキュリティを実装できます。

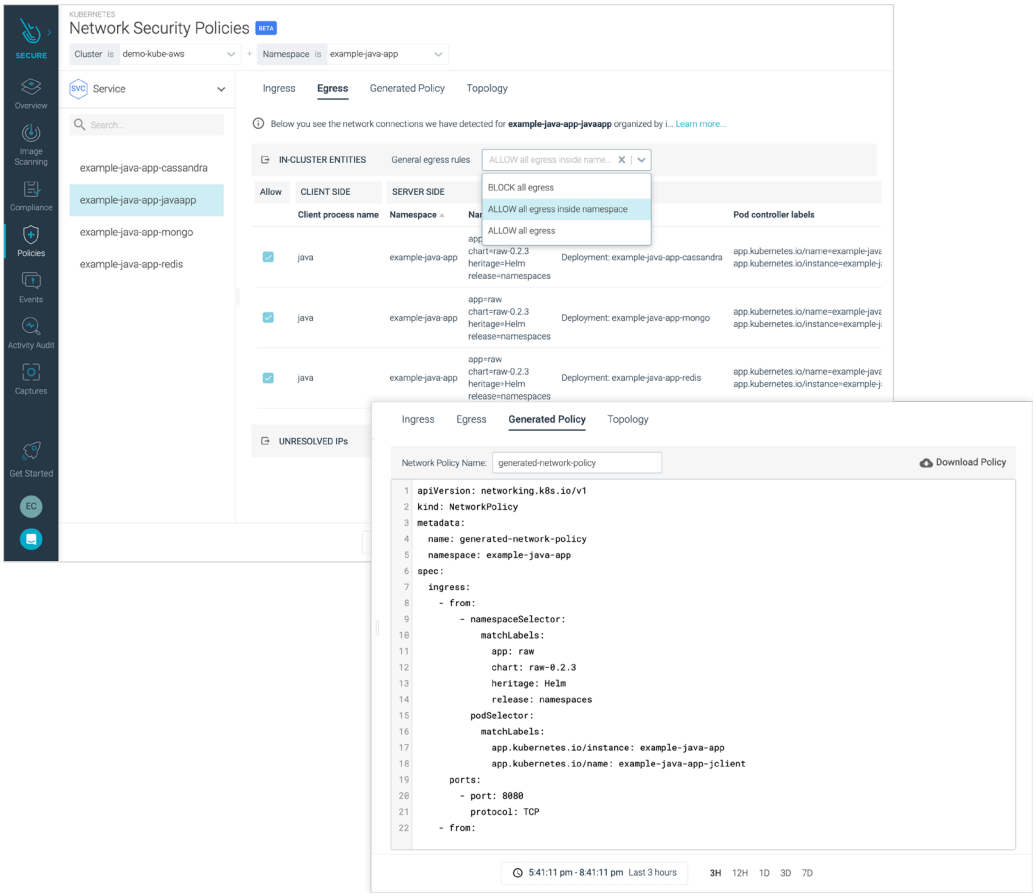
Sysdigが追加する機能

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オプションを提供します。ネイティブコントロールでは、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、より優れたパフォーマンス、信頼性、およびセキュリティを確保できます。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が困難であるという課題があります。Sysdigを使うと、これらの障壁を取り除き、Kubernetesの制御によるゼロトラストネットワークセキュリティの実装がより簡単に行えるようになります。

Sysdig Secureは、システムコールに関する可視性を通じて、EKS Pod、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知します。データはKubernetesのコンテキストとラベルで自動的にタグ付けされ、Kubernetesネットワークポリシーを実装する際のエクスペリエンスを簡素化するために使用されます。



動的なトポロジーマップにより、アプリケーションと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のドリルダウンが行えるようになります。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絞り込むことができます。Sysdigは、Kubernetesクラスターにポリシーを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作成できます。このAudit Tap機能により、クラウドチームは、ラベルを含むコンテキストを完全に可視化しつつ、きめ細かなレベルでネットワークアクティビティを調査できるようになります。NISTやPCIなどの規制を受ける企業は、この機能をネットワークセグメンテーションと組み合わせて活用することで、コンプライアンス要件を満たすことが可能となります。

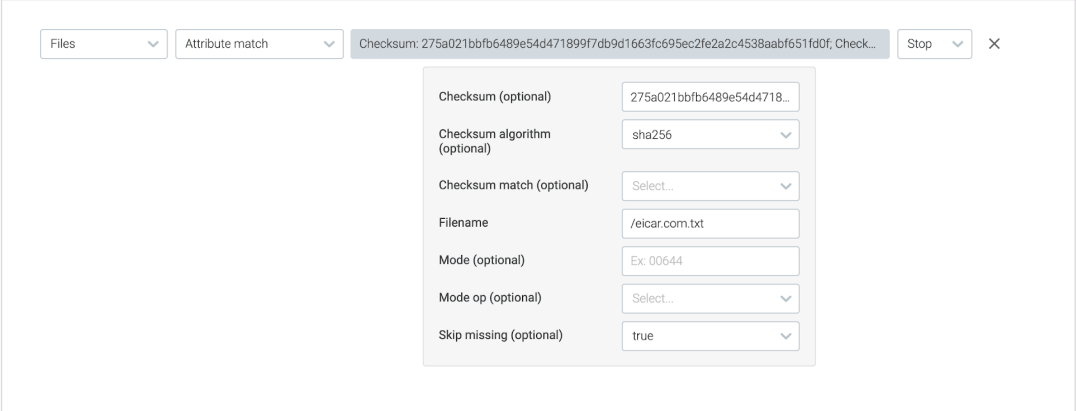
Sysdigを使用して、コミュニティによって吟味されたオープンで標準ベースのアプローチに基づくゼロトラストネットワークセキュリティを実現すると、Kubernetesが強制力を提供するようになるため、パフォーマンス、信頼性、およびセキュリティの向上を実現できます。これにより、中間者（man-in-the-middle）による強制の仕組みが不要になります。Sysdigは、Kubernetesの専門知識を持たないチームに対して使いやすいインターフェイスを提供し、「ガードレール」を自動化することで、AWSユーザーの時間を節約し、ネットワークセキュリティのリスクを低減します。

ファイル整合性監視（FIM）

ファイル整合性監視は、機密性の高いファイルに関連するすべてのアクティビティを可視化します。アクティビティが悪意ある攻撃であるか、計画外の運用活動であるかに関わらず、FIMは、重要なシステムファイル、ディレクトリの改ざん、不正な変更を検知するために使用されます。

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それらを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ない場合、早期にビルドを中止できます。ファイル整合性監視ポリシーでは、次のことが可能です。

- ファイルが存在するか、または存在しないかをチェックし、その条件に基づいて警告を発行すること。
- 特定のファイルをそのSHA256ハッシュと照合して検証すること。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を立てること。
- ファイルのパーミッションを検証すること。たとえば、ファイルが予期しない場所に実行可能ビットを持つ場合、アラートを発行できます。
- 正規表現に基づいてファイル名をチェックすること。
- コンテンツを検査し、公開されたパスワードやクレデンシャルの漏洩がないかどうか調べすること。



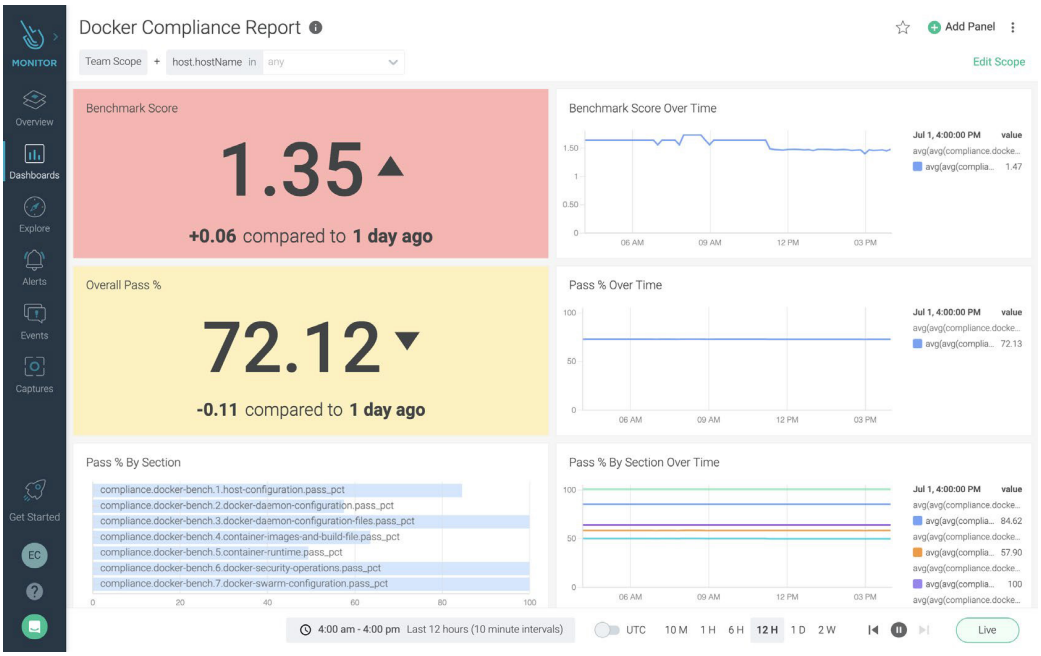
また、ファイルシステムに対する疑わしい変更に警告するFIMポリシーを実行時に実装することもできます。強力なセキュリティ体制を強化するためにルールとして含めるべき、一般的なファイル整合性監視のチェック対象としては、次のものが挙げられます。

- ファイルまたはディレクトリの作成または削除
- ファイルまたは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、継承などのファイルまたは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に対する変更
- コンテナのパスの下にあるファイルの変更
- bash履歴の削除

Sysdigプラットフォームは、堅牢なレポートを生成するだけでなく、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とダッシュボードに変換します。これにより、内部および外部のコンプライアンス監査チームは、自社のセキュリティ状況を分析し、パターンや傾向を迅速に可視化し、コンプライアンス状況について貴重なインサイトを得ることができます。これにより、次のことが可能となります。

- 現在のセキュリティ状況を過去の任意の時点と比較すること。
- アプリケーションと環境全体のリスクとコンプライアンスの状況を把握すること。

- コンプライアンスチェックが許容されたポリシーを下回った場合に警告を出すこと。
- AWSコンテナクラスター全体の構成ドリフトを検知すること。



ランタイムセキュリティ

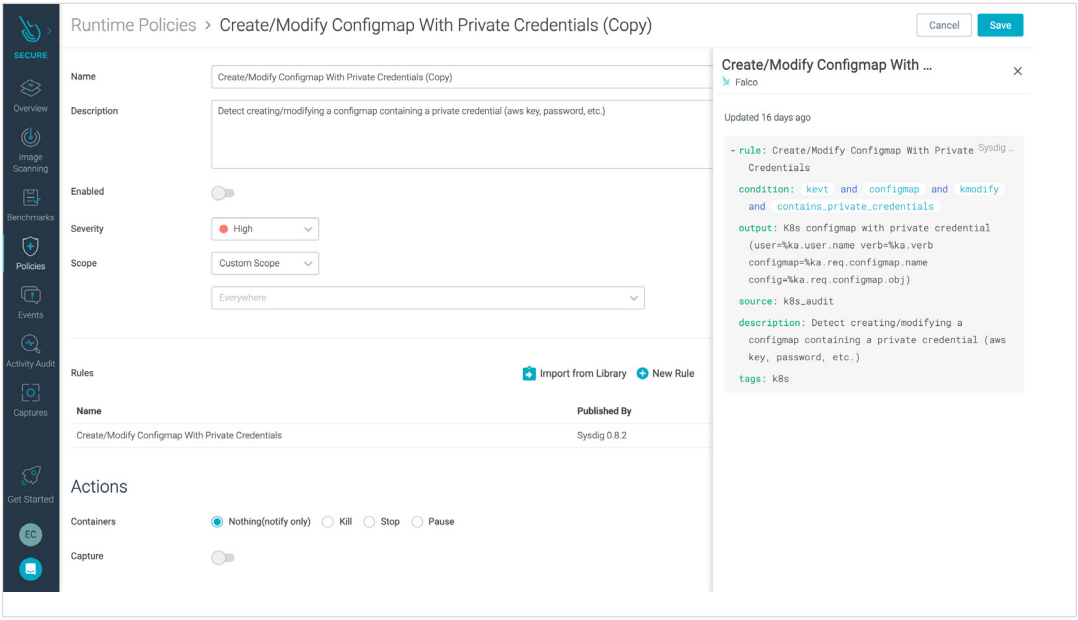
セキュリティ監視

AWSのクラウドとコンテナサービスの監視とセキュリティの両方に関する可視性を確保することは、トランスフォーメーションを成功させるために必要となります。たとえば、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における異常な偏差によってさらに詳細に説明できるかどうかを知る必要があります。

さらに、運用開始後は、最小の権限とアクセスパーミッションでアプリケーションを構成することで、リスクを低減する必要があります。同時に、ワークロードの動作を観察して異常な動作を探し、CI/CDやレジストリスキャンで検知できなかった脅威や攻撃をブロックするランタイムポリシーを作成維持できるようにする必要があります。

脅威の検知

Sysdigは、CNCF Falcoプロジェクトのオープンソース検知エンジンを活用することで、ホストやコンテナ上の異常なアクティビティを実行時に監視します。また、AWS CloudTrailのログや、KubernetesやEKSマネージドサービスを使用する際のオーケストレーションレイヤーからのアクティビティを取り込んだ上で、それらを監視できます。



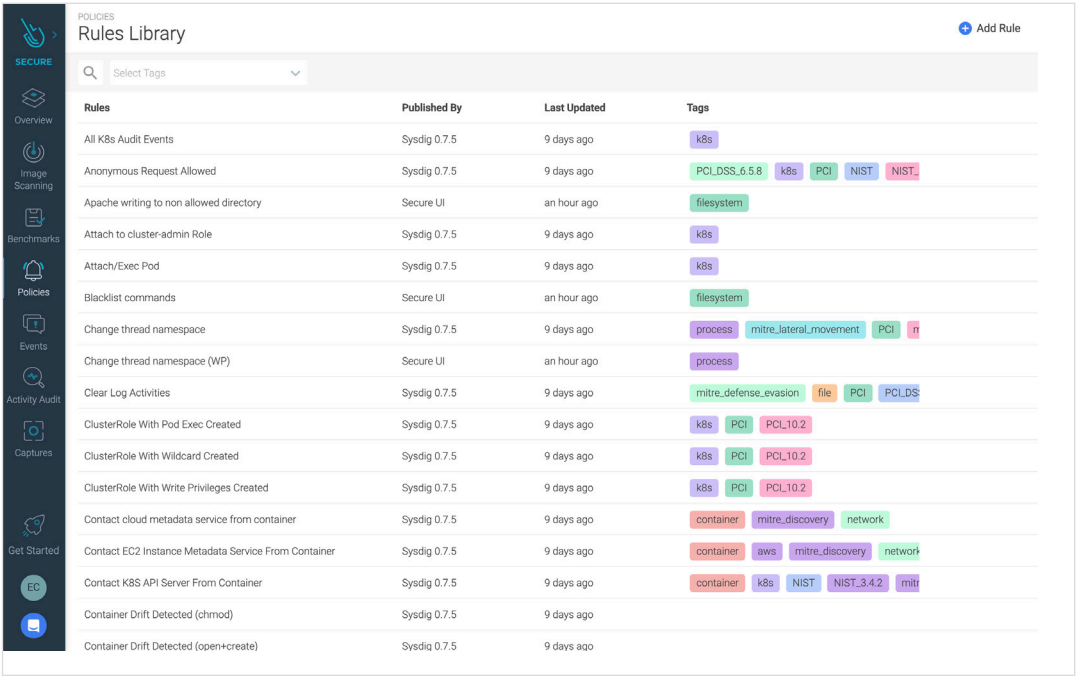
EKSからのKubernetesサーバーAPIイベントの取り込みについての詳細は、「こちら」をご覧ください。

CI/CDプロセス中やAWS Elastic Container Registryからコンテナを一度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知されますが、いくつかのセキュリティ脅威は、その性質上、実行時にのみ顕在化するものです。これには次のものが含まれます。

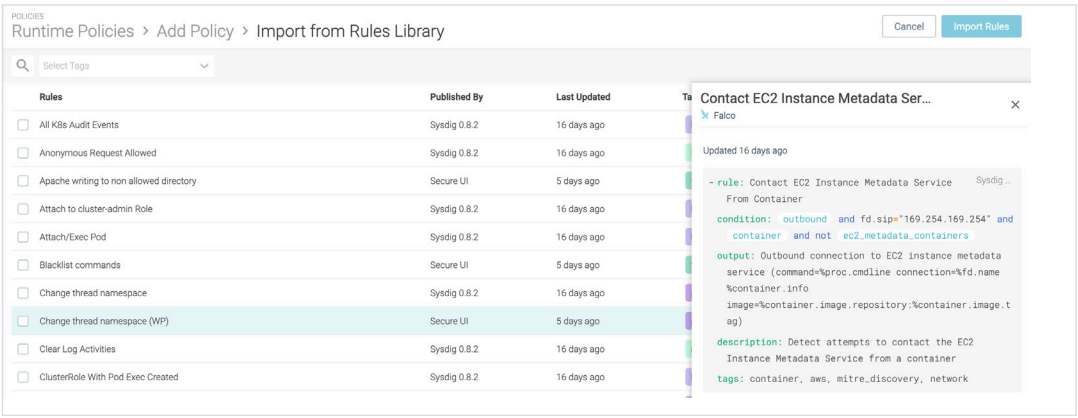
- ゼロデイ脆弱性、自社ソフトウェア固有の非パブリックな脆弱性
- ソフトウェアのバグによる異常な動作やリソースの漏洩
- 内部での権限昇格の試み、または隠蔽された/組み込まれたマルウェア

デフォルトのポリシーに加え、200以上のルールが用意されており、要件に合わせたセキュリティのカスタマイズ作業を簡素化できます。Sysdig Secureのポリシーを使用すると、Fargate、ECS、EKSなどのAWSクラウドやコンテナサービスに対する脅威を検出するためのランタイムセキュリティを簡単に実装できます。これには次のものが含まれます。

- コンテナの規制コンプライアンス基準に対応したコンテナランタイムの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
- 最も広範なコンテナ攻撃のランタイム検知：クリプトマイニング、機密流出、コンテナ隔離違反、ラテラルムーブメント
- 予期せぬプロセスアクティビティ、アウトバウンド接続、端末シェルセッションのセキュリティ監視
- AWSクラウドサービス全体の疑わしいアクティビティを特定するCloudTrail検知ルール

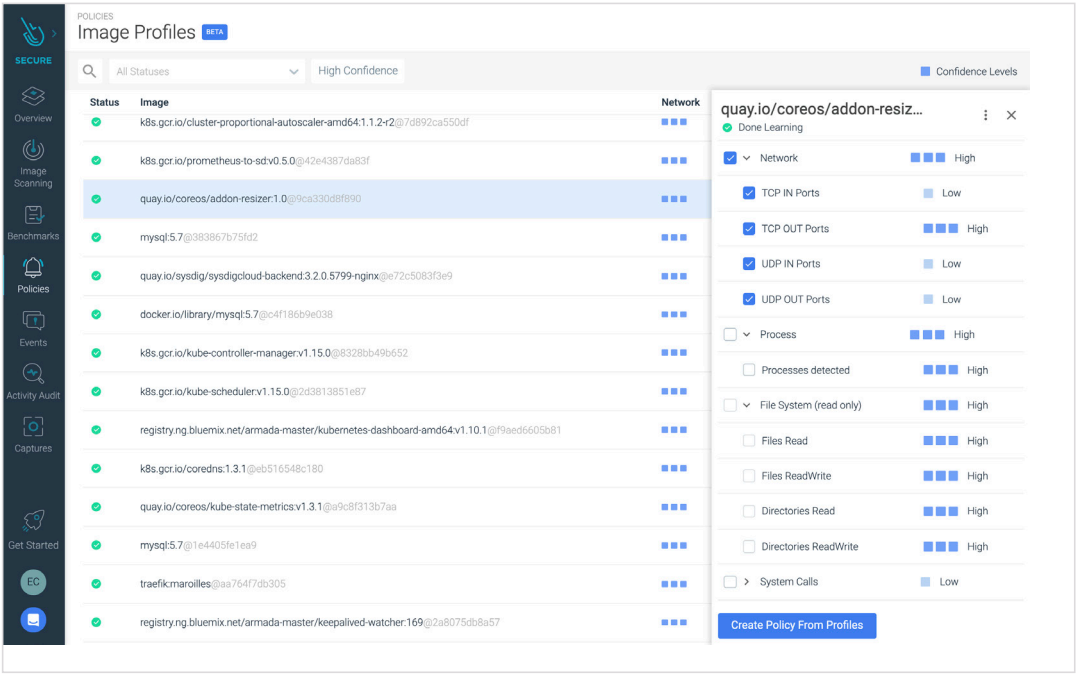


オープンソースのFalcoを採用した拡張可能なポリシーエンジンにより、運用およびセキュリティチームは、ビジュアルインターフェイスを通じて独自のルールのカスタマイズや作成を通じて、要件に合ったきめ細かいポリシーを構築できます。コミュニティをソースとする厳選されたFalcoルールは、Cloud Native Security Hubを通じて利用可能です。



ランタイムイメージプロファイリング

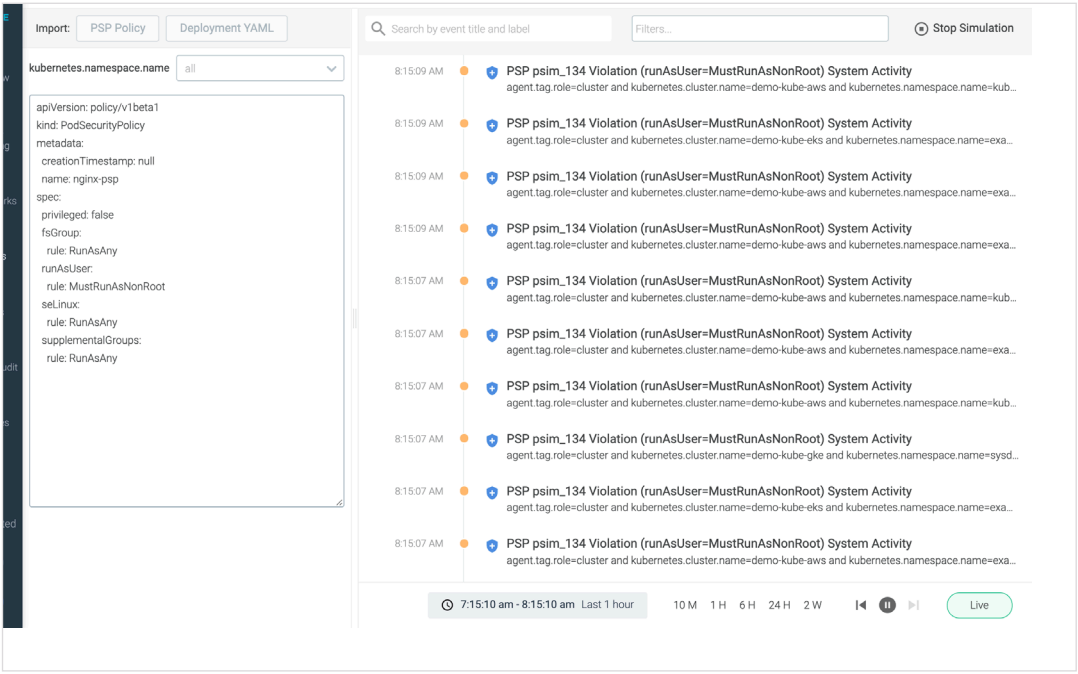
大規模環境におけるランタイムセキュリティの構築維持の負担を軽減するために、Sysdig Secureはランタイムイメージプロファイリングを搭載しています。イメージプロファイリングは、コンテナランタイムの挙動を自動的にモデル化、分析、学習することで、包括的なコンテナランタイムプロファイルを作成し、自動的にポリシーを構築します。これには、ECS、EKS、クラウドラベルなどのさまざまなメタデータを使ってそれらをリッチ化しつつ、kube-apiserverのアクティビティやシステムコールを分析することが含まれます。このアプローチにより、機械学習による異常検知を強化し、脅威が伝播する前にそれらをブロックできるようになります。



Kubernetesのネイティブコントロールによる脅威対策

Sysdigは、Pod Security Policies（PSP）などのKubernetesのネイティブコントロールを使用して脅威を防止します。Kubernetes Policy Advisorは、PSPの生成を自動化し、導入前に検証を行うため、適用時にアプリケーションを破壊することはありません。これにより、ユーザーは本番環境において迅速かつ容易にPSPを採用できるようになります。また、PSPは、ホスト上のすべてのアクションをインターセプト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ずに脅威を防止するKubernetesのネイティブコントロールメカニズムを提供します。

Sysdig Secureでは、PSPのようなKubernetesネイティブコントロールをエンフォースメントに活用しています。Sysdigのランタイムセキュリティ機能に関する詳細は、ブログ記事『Pod Security Policies in production with Sysdig's Kubernetes Policy Advisor（SysdigのKubernetes Policy Advisorを使った本番環境でのPodセキュリティポリシー）』をご覧ください。



Sysdig Secureを利用することで、運用および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、ボンネットの下で起きていることをより詳細に管理できるようになるため、透明性と保証を高めることができます。

AWSクラウドのセキュリティポスチャー管理

Sysdigが実施した脅威に関する調査では、クラウド、ワークロード、コンテナを一元管理することで、セキュリティ侵害の大半で使用され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を迅速に行えるようになることが示されています。

複数の異なるクラウドおよびコンテナ用のセキュリティツールを使用すると、セキュリティ運用が複雑になります。なぜなら、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は、異なるデータソースの相互関連付けを手動で行う必要があるからです。Sysdigは、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と、CSPM（Cloud Security Posture Management）およびクラウド脅威検知を1つのプラットフォームで組み合わせて提供します。

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、攻撃者がどこから侵入を開始したか、そして環境内を移動する際に取った各ステップを正確に把握できます。

クラウドアセットディスカバリー

クラウド資産は境界の制約を受けずに動作し、APIやその他のコネクタを通じてAWS環境に継続的にリソースがもたらされるため、どの資産が実際に環境と対話しているかを知ることが必要です。AWS環境全体にセキュリティを適用するには、これらすべてのデータソースがどのように接続し対話しているかについてのインテリジェンスを含む、資産のリスト（インベントリ）が必要となります。

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から構成され、APIを通じてアクセス可能です。各サービスには、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など、クラウド環境内の他のリソースへの接続が存在します。

ほとんどの企業や組織では、これらのリソース、それらの関係、および構成を特定するために、手作業による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動管理は拡張性がないため、これらのアセットとその動作のリスト（インベントリ）を作成し、追跡するための自動化サービスが必要となります。

AWSが提供するもの

AWS Application Discovery Servicesは、オンプレミスサーバーやその他のクラウドアセットに関する使用状況や設定データを収集します。これはAWS Migration Hubと統合されており、新しいアセットが統合や他の接続形態を通じて環境に入り込む際に、それらのアセットを即座に特定できます。Application Discovery ServicesのAPIを使用すると、ユーザーは検知されたすべてのサーバーのシステムパフォーマンスと使用率データにアクセスできます。

Application Discovery ServiceのAPIを使用すると、検知したサーバーのシステムパフォーマンスと使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すると、AWSでこれらのサーバーを実行するコストを計算できます。さらに、サーバー間に存在するネットワーク接続に関するデータをエクスポートできます。この情報は、サーバー間のネットワークの依存関係を決定し、移行計画のた

めにそれらをアプリケーションにグループ化するのに役立ちます。

Sysdigが追加する機能

クラウドセキュリティチームは、Sysdigを使用して、AWSクラウド環境全体で実行されているシステム、アプリケーション、サービス、スクリプトを自動的に検知し、セキュリティ体制を管理できます。これにより、チームは、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、機密データ（顧客データ、コンプライアンス規制の対象データなど）がどこに保存され、処理されているかをより深く理解できるようになります。

この機能は、クラウドインフラストラクチャーを保護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、AWSアカウントで稼働するリソースとアセット、および各リソースとプロジェクトにロールアップされるすべてのアセットをリアルタイムにダッシュボードで表示します。現在の運用状況を把握することで、最も深刻な脅威が存在するサービスに優先順位を付け、修復を加速させることができます。

Sysdigでは、各AWSリソースやプロジェクトに対してドリルインすることで、対応する設定を確認できます。Sysdigは、他のシステムからのデータと共に、各AWSアカウント内のアセットを識別し分類することで、クラウド内のすべてのサービスに関する1つの「信頼できる唯一の情報源」を作成します。

アセット管理は、構成コンプライアンスにおける重要な要素です。クラウド環境は動的でありかつ複雑です。設定や変更を手動で追跡検知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、継続的にチェックを実施することで、設定がこれらの特定のコンプライアンスの枠組みの要件を満たしていない場合にはアラートを発行します。

Sysdigのユーザーは、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できるため、イベント情報の相互関連付けを手動で行う必要性が減少します。Sysdig SecureはKubernetesのアクティビティに関する関連するコンテキストも提供するため、ユーザーは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きているかをより深く理解できるようになります。

クラウドインフラストラクチャーエンタイトルメント管理

アイデンティティとアクセス管理（IAM）の設定ミスは、クラウドセキュリティにおける最も一般的な懸念事項の1つです。アクセス制御やアクセス許可が寛容すぎると、攻撃者に悪用されて不正にアクセスされる可能性があります。その結果、環境内でのラテラルムーブメントが発生し、機密データが流出する可能性があります。

クラウドのパーミッションリスクを防止するために、クラウドチームはCloud Infrastructure Entitlements Management (CIEM) ソリューションを活用できます。CIEMツールは、過剰なパーミッションや未使用のパーミッションを持つアカウントやロール、および未使用のアカウントの検索に特化しています。クラウド環境で利用できるパーミッションは粒度が細かいため、CIEMツールは適切なアクセス設定を実現するためのカギとなります。ユーザーやシステムがアクションを実行するために必要なものを慎重に与えることは、クラウドセキュリティの基本です。この「最小権限」の概念は、データ漏洩のリスクを回避し、権限昇格を抑制し、ラテラルムーブメントをブロックするための重要なベストプラクティスとなります。

AWSが提供する機能

AWS Identity and Access Management（IAM）Access Analyzerは、新規または更新されたリソースポリシーの監視と分析を行い、潜在的なセキュリティ上の影響を理解するのに役立ちます。リソース許可を展開する前にAccess Analyzerの結果をプレビューできるため、ポリシーの変更が意図したアクセスのみを許可することを検証できます。これにより、リソースのアクセス許可を導入する前に、ポリシーがパブリックアクセスやクロスアカウントアクセスにどのように影響するかをプレビューできます。

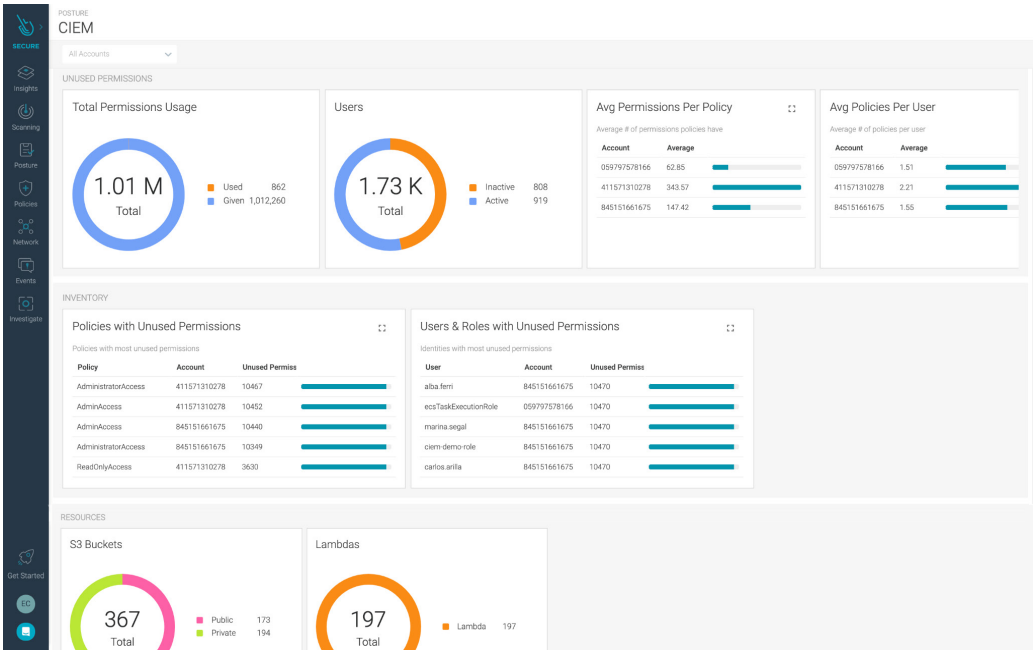
Sysdigが追加する機能

Sysdigには、サーバーレス機能を含むAWSアカウント、ユーザー、サービス全体のアクセス権限を包括的に把握できるクラウドインフラストラクチャーエンタイトルメント管理が含まれています。Sysdig Secureは、実行されたクラウドコマンドの監査ログを分析し、このアクティビティをアカウント内のポリシー、ロール、ユーザーと相互に関連付けるため、この同じ情報を使用して、権限使用のプロファイルを作成できます。これにより、お客様は、アクセス設定の監査を簡素化し、コンプライアンス要件に対応できるようになります。

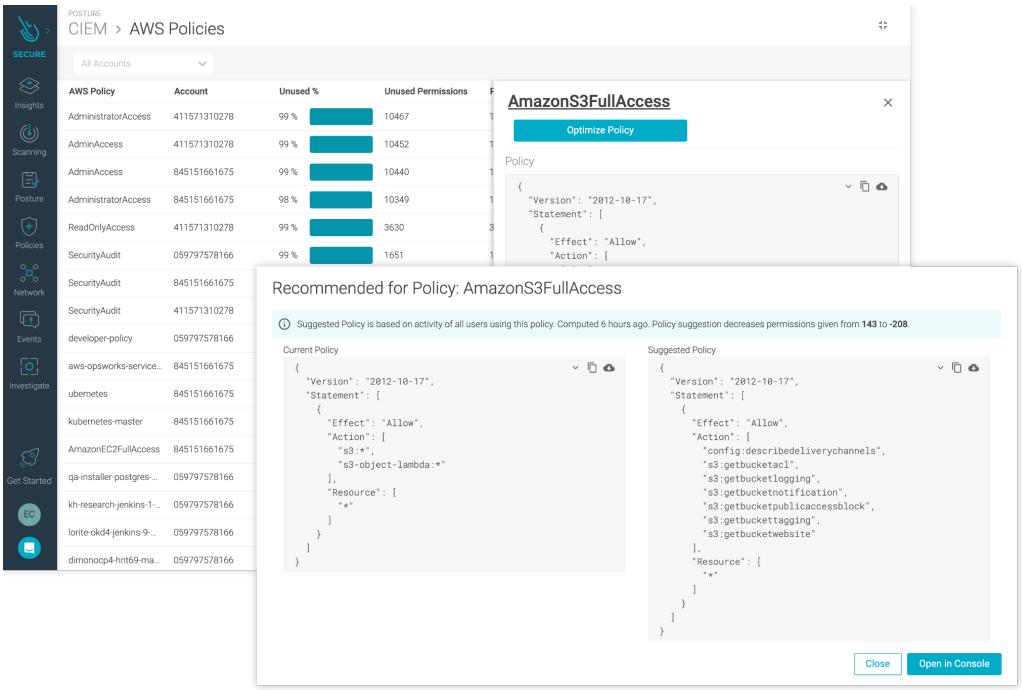
Sysdig CIEMの可視化機能により、実際のパーミッションの使用状況を把握し、過度に寛容なアクセス権や古いアクセス権が存在している場所（クレデンシャルの不正使用のリスクがある場所）を特定できます。ダッシュボードは、次のような情報を提供します。

- 与えられたパーミッションと使用されたパーミッションの合計数
- 非アクティブなユーザー数と、削除を検討すべきユーザー数
- ポリシーごとのパーミッションの平均値とユーザーごとのポリシーの平均値
- 未使用のパーミッションのワーストケースを持つポリシー、ユーザー、およびロール

これらのメトリクスを使用することで、自社のIAMセキュリティ体制の強化に向けた進捗状況を確認できます。



Sysdig Secureは、付与されたクラウド権限と実際に必要な権限を分析することで、IAMの設定を改善できます。このソリューションを使うと、「必要十分な」権限と自動提案ポリシーを提供できるようになります。このポリシーを使うことで、最小権限アクセスを数分で管理して実施できるようになります。



静的な構成管理

アプリケーションをはじめとするクラウド上のシステムは、セキュリティを重視して設計されている場合であっても、クラウド環境の変化に伴い、当初設定した内容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、本番稼動しているアプリケーションを監視するための設定にセキュリティリスクが生じる可能性があります。したがって、重要なのは、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しつつ、組織のAWSアカウントに対応するセキュリティ体制を維持するために、AWSリソースに構成管理を適用することです。

クラウドのワークロードとアプリケーションの開発が急速に変化する中、アプリケーションの機能は絶えず進化しています。その結果、手動で追跡できない構成の変更が発生しています。AWSとSysdigの連携により、クラウドユーザーはAWSアカウントにおける継続的なクラウド構成の監視と監査レポートを利用できるようになり、その結果、AWSインフラストラクチャーのネットワーク、ストレージ、ユーザーアクセス、ログの側面からコンプライアンス違反を検知することが可能になります。

AWSが提供する機能

AWS Configは、AWSリソースの構成に関する継続的な評価、監査、およびレポーティングを実行します。環境のAWSリソースの構成を監視し、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できます。管理者は、構成の変更とそれが他のAWSリソースとの関係に与える影響を確認し、変更の履歴の推移を分析できます。ユーザーは、一定期間内にワークロードがどのような構成で稼働しているかを確認し、AWSリソースの変更がいつ（環境内のどこで）構成に影響を与えたかを判断できます。

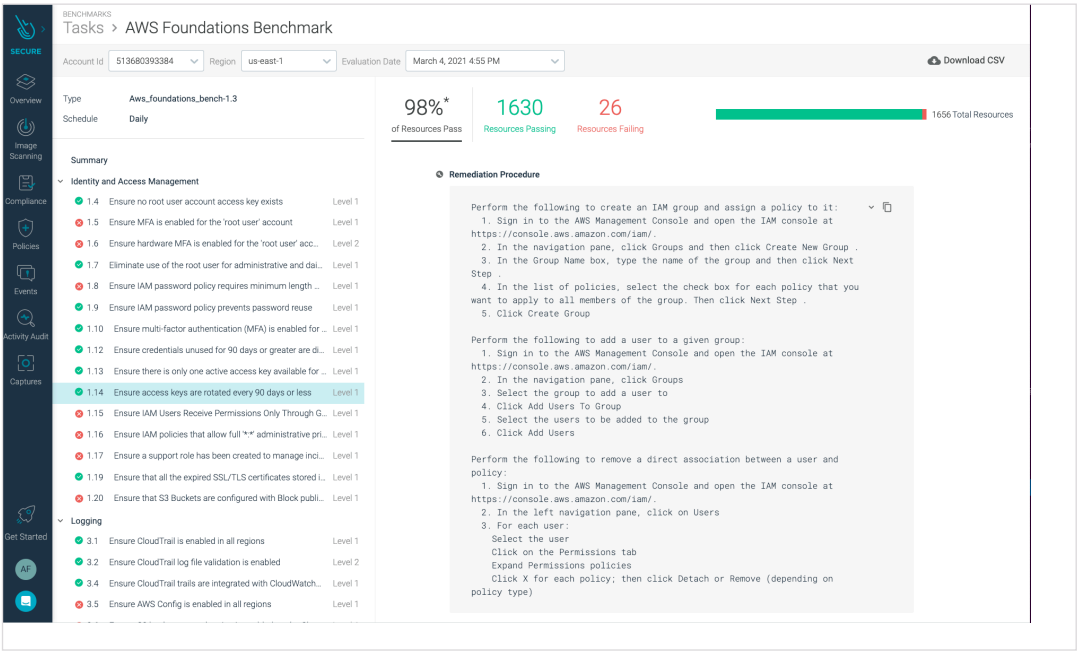
AWS Configを有効にすると、指定されたアカウントに存在するサポートされているAWSリソースを検知し、各リソースの受け入れ設定レポートを生成します。これにより、ユーザーの環境にあるサポートされているすべてのリソースの構成項目が作成されます。

Sysdigが追加する機能

AWSアカウントにワークロードが増え、アプリケーションの統合が進むと、イベントや操作の痕跡の量が圧倒的に多くなります。スケーラブルな自動化されたアプローチなしには、分析は不可能です。Sysdig Secureは、リスクの高い構成設定を特定し、クラウドとコンテナ環境の現在のセキュリティ体制を可視化できます。これにより、公開された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設定ミスの検知が容易になり、設定ドリフトがあるかどうかを迅速に判断できるようになります。

Sysdigは定期的にAWS Foundations CIS benchmarkに照らしてクラウド構成を分析します。これは、AWSアカウントに関する精選されたチェックのコレクションであり、どのサービスや構成がセキュリティ上の課題を提示しているかを通知するものです。また、クラウド資産全体の構成の問題を修正するための適切なステップを実行するのに役立つガイダンスも提供します。

Sysdigは、セキュリティチームやDevOpsチームの視点から、読みやすくコンテキストに応じた形式で構成に関するインサイトを提供するほか、監査を支援することで、コンプライアンスと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提供します。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作業となっています。



AWS CloudTrailのログを利用した脅威検知

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のイベントとしてログに記録されます。これには、AWS Management Console、AWS Command Line Interface、およびAWS SDKとAPIへのあらゆる変更が含まれます。

AWSが提供する機能

CloudTrailから利用できるイベント履歴は、セキュリティ分析、リソース変更の追跡、およびトラブルシューティングを簡素化します。CloudTrailが提供する情報を使用して、AWSアカウントの異常なアクティビティを検知し、運用分析とトラブルシューティングを簡素化できます。CloudTrailを使うと、AWSリソースのセキュリティを脅かすアカウントのアクティビティを追跡して対応できるようになります。

また、AWS GuardDutyを活用することもできます。これは、AWSのワークロード、アカウント、APIコール、S3バケットに保存されたデータにおける悪意ある活動や異常な動作を監視する脅威検知サービスです。このサービスは、CloudTrailの監査ログに基づき、セキュリティ上の問題を示唆するような異常な活動を特定します。

Sysdigが追加する機能

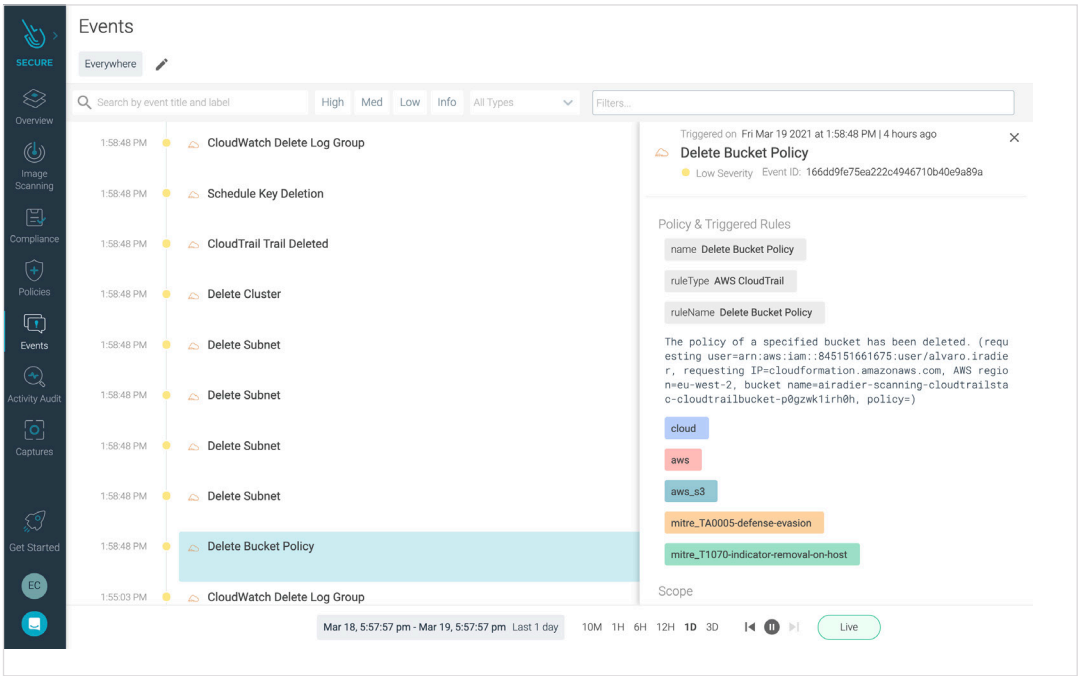
インフラストラクチャーが成長するにつれて、CloudTrailから利用できるイベントと運用ログの量は、手動での分析と対応が不可能なサイズにまで増加する可能性があります。脅威への対応の遅れは、潜在的に大きな影響を及ぼす可能性があります。

Sysdigは、オープンソースのFalco脅威検知に基づく柔軟なセキュリティルール群を使用することで、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。Falcoは、コンテナやKubernetes環境全体で脅威を検知するエンジンと同じものです。

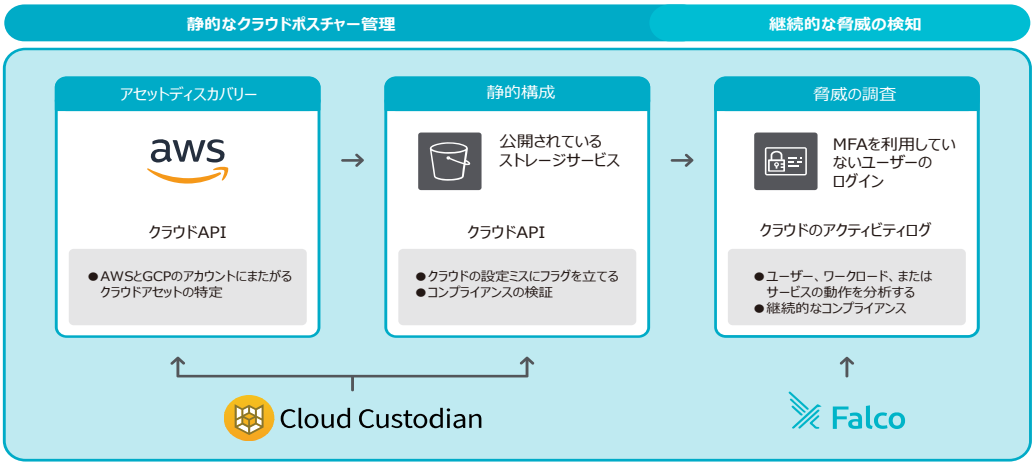
SysdigとCloudTrailの統合により、事前に設定されたポリシーを使用したり、予期しないアクティビティにアラートを出すために独自の検知を作成したりできます。100以上のコミュニティ主導の、すぐに使えるFalcoルールの包括的なセットを活用することで、時間を節約できます。さらに、DevOpsとセキュリティチームは、AWS環境を離れることなく、AWS Security Hubで直接イベントを確認することで、迅速に調査結果を得ることができます。

Sysdig Secureは、一度設定すると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、疑わしいクラウドの活動やイベントを継続的に検知しレポートします。その使用例を下記に示します。

- 不審なIAMアクティビティや異常な権限変更を探す。
- 予期しない動作やリモートでのコード実行がないか、プロセスの実行パターンを検知する。
- クレデンシャルの盗難、特に寿命の長いクレデンシャルや高権限のクレデンシャルを探す。
- クラウドリソース（S3など）、仮想サーバー用のインフラストラクチャーポート、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設定変更を確認する。
- 意図しない情報の露出による機密データの漏洩を特定する。
- 過去のインシデントのデータを調査し、パターンを検知する。



CloudTrailの対応サービス一覧は、AWSのWebサイトで順次公開されています。



AWSコンテナサービスの監視

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のために重要です。コンテナとクラウド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と開発を容易にし、より迅速なイノベーションと新機能の市場投入までの時間の短縮を可能にします。アプリケーション内で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困難になることがあります。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インフラストラクチャーを横断して移動できます。Kubernetesのオーケストレーション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把握する上で重要です。

AWSが提供する機能

AWSでは、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況を監視観測するサービス「Amazon CloudWatch」を提供しています。

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変化への対応、リソース利用の最適化、および運用状況の統一見解を得るためのデータと実用的なインサイトを提供します。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、AWSリソース、アプリケーション、およびAWSとオンプレミスサーバー上で実行されるサービスの統合ビューを提供します。CloudWatchは、環境内の異常な動作を検知し、アラームを設定し、ログとメトリクスを並べて可視化し、自動化されたアクションを実行します。さらには、問題のトラブルシューティングを行うほか、アプリケーションをスムーズに稼働させるためのインサイトを提供します。

また、Prometheusのメトリクスを CloudWatchで収集することで、アプリケーションのパフォーマンス低下や障害をより迅速に監視し、トラブルシューティングを行い、アラートを発行することも可能です。

Sysdigが追加する機能

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できます。オープンソースをベースに構築されており、急速に変化するコンテナ環境に対してディープな可視性を即座に提供します。Prometheusのメトリクスに加えて、クラウドやKubernetesのコンテキストに富んだ実際のシステムコールから得られるきめ細かいデータを使用することで、問題をより迅速に解決できます。Sysdig Monitorを使うと、ハイブリッドおよびマルチクラウドモニタリングのためにチーム間でデータを統一することで、サイロを除去できるようになります。

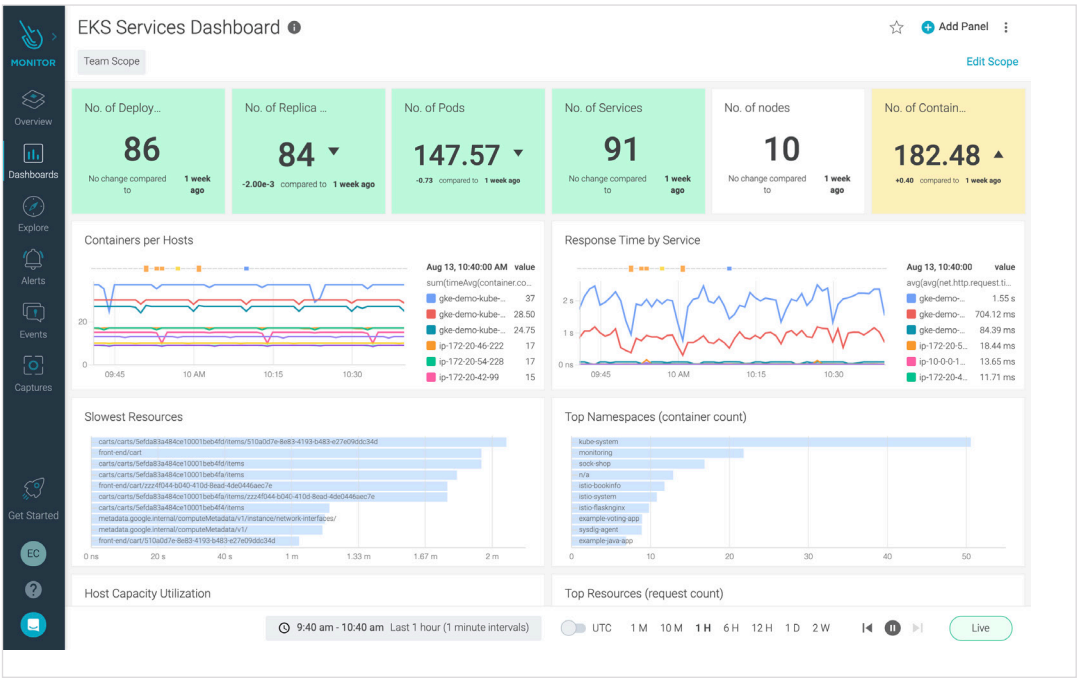
Sysdig Monitorは、Prometheusのオープンスタンダードの利点を損なうことなく、クラウドチームが独自の監視システムを設定管理する負担を取り除くような、スケーラブルなマネージド型のPrometheusサービスを提供します。Sysdig Monitorは、Prometheus監視統合の自動検知と導入支援を提供するほか、事前設定されたダッシュボードとアラートを提供します。

Prometheus Query Language（PromQL）とPromQL Explorerのサポート Sysdigは、クエリを使用して平均検知時間（MTTD）を短縮するために、メトリクスとの対話を簡素化します。さらに、PromQLライブラリは、監視コミュニティから人気のあるクエリを発見し、本当に重要な情報にアクセスするための新しい方法を学ぶのに役立ちます。

Kubernetesとコンテナ監視

Sysdigを利用することで、クラウドチームは、クラスター、導入、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、健全性とパフォーマンスの詳細情報を受け取ることができます。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に対するディープな可視性により、チームはコンテナ展開の複雑さを管理できます。これにより、次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、アプリケーションを詳細に可視化し、健全性とパフォーマンスを監視する。
- Kubernetesのオーケストレーションコンテキストを使用し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する。
- 過剰なリソースを消費しているPodを特定し、キャパシティの制限を監視する。
- アプリケーションのオートスケーリング動作を監視し、予期せぬ課金を抑制する。
- クラスターとクラウド間でキャパシティを最適化することにより、コストを削減する。

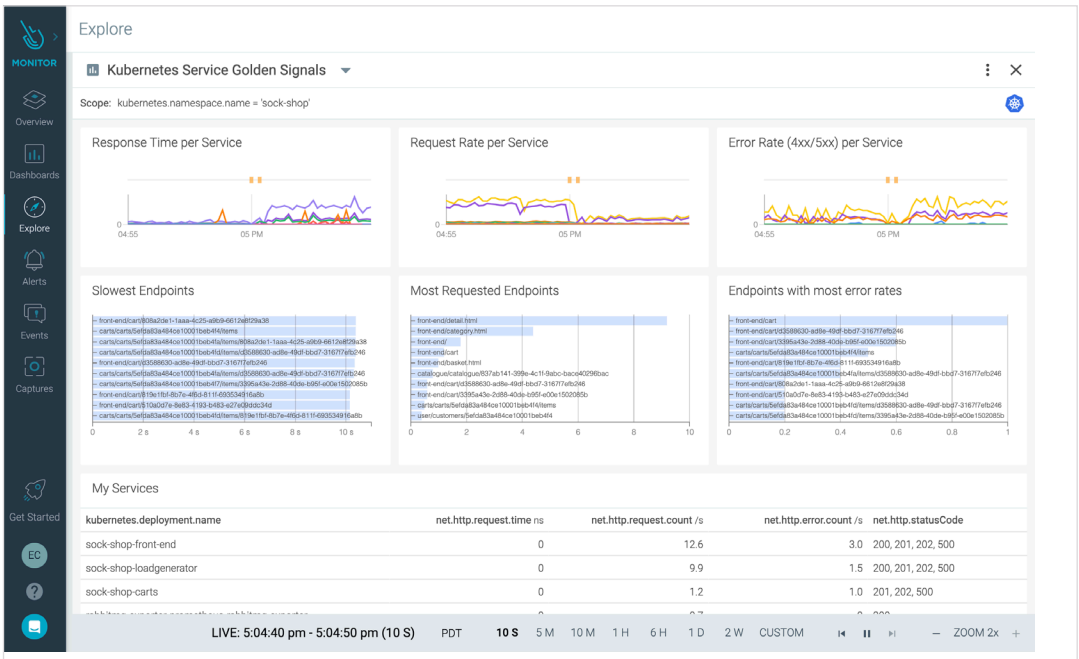


アプリケーションとサービスの監視

遅延、エラー、トラフィック、飽和の各メトリクスは、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、そのサービスと相互作用してい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ています。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覆い隠してしまうような罠を避けることで、時間を節約できます。

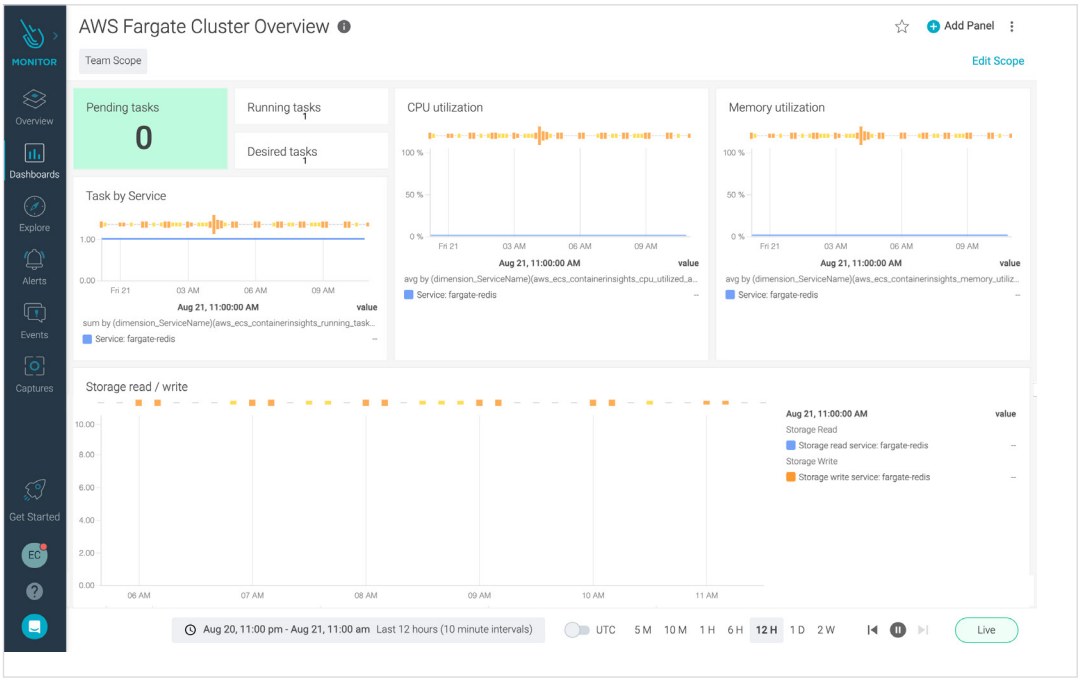
Sysdig Monitorでは、次のことが可能です。

- アプリケーションの可用性とセキュリティに関する「信頼できる唯一の情報源」により、インサイトまでの時間を短縮し、チームは問題を迅速に解決すること。
- コンテナの詳細な可視化と、Kubernetesとクラウドのコンテキストに基づいたきめ細かいメトリクスにより、アプリケーションのパフォーマンスを向上させ、問題を迅速に解決すること。
- すぐに使えるダッシュボードを使用して、クラウドサービス、データベース、およびAWS環境のその他の主要コンポーネントのメトリクスを観察すること。
- 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。
- チーム、SSO、RBACなど、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適用することで、リスクを低減すること。
- Prometheus とPromQLの完全な互換性により、クラウドスケールで既存の開発者への投資を活用すること。
- Prometheus互換のエクスポーター、ダッシュボード、アラートを使用して、数百のアプリケーションやサービスに監視を拡張すること。
- 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向けの、精選、文書化、サポートされたモニタリング統合を使用することで、より迅速に生産性を高めること。



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、またAmazon CloudWatchでPrometheusを簡単に利用できるようになります。Sysdig Monitorは、Prometheus経由でAWS CloudWatchのメトリクスを抽出し、SysdigやGrafanaダッシュボードを用いて可視化することが可能です。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から、AWSサービス用の吟味されたPrometheusエクスポーター、ダッシュボード、アラート、記録ルールに関する、厳選されたレポジトリが利用できます。

ドキュメントによる検証済みのサポートがあることで、Prometheus統合の調査やメンテナンスに費やす開発者の時間を削減し、数週間の労力を節約できます。AWSとの統合の例としては、AWS Fargate、AWS Lambda、AWS Application Load Balancer (AWS ALB) 、AWS Elastic Load Balancer (AWS ELB) 、Amazon Simple Storage Service (Amazon S3)のサポートが挙げられます。



サービスメッシュの可視性

マイクロサービスの管理をより効率的かつ容易にするために、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基盤の次の中核となる構成要素となっています。サービスメッシュは、サービスの発見、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、監視することを支援します。

AWSが提供する機能

AWS App Meshは、ECS、EKS、Fargateのため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の監視と制御を容易にします。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提供し、アプリケーションの高可用性を保証します。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、単一のビューと制御の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おり、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を持っています。

Sysdigが追加する機能

SysdigはAWS App Meshをサポートしており、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さらに可視化し、セキュリティプロファイルやサービスメッシュ全体の健全性をさらに詳細に把握できるようになります。Sysdigを利用することで、AWS App Meshのユーザーは、サービスメッシュのパフォーマンスを監視するだけでなく、インフラストラクチャー全体のパフォーマンスやセキュリティの指標を確認することができ、コンテナ化した環境にさらなる制御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自動的にメトリクスをスクレイピングする機能により、AWS App Meshの監視を強化します。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ストラクチャー全体から収集してリッチ化する膨大な量のメトリクスやイベントデータと相互に関連付けることができます。

コンテナフォレンジックとインシデント対応

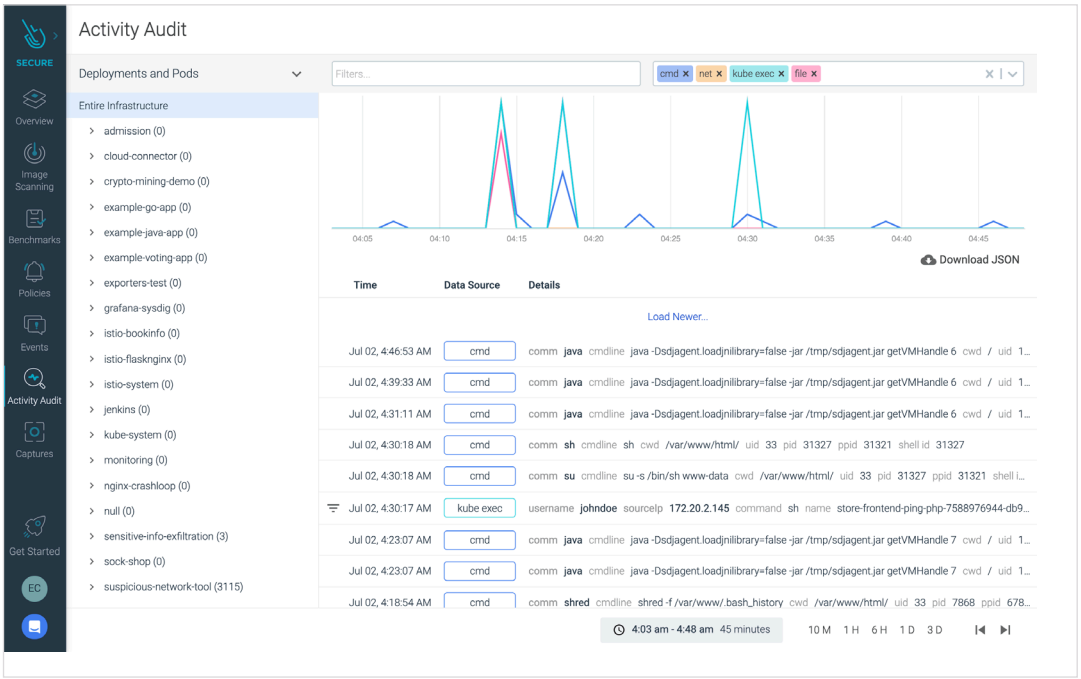
問題のトラブルシューティングやセキュリティインシデントの事後分析を行う際、典型的な課題の1つは、コンテナが破壊されると関連情報がすべて消えてしまうことです。

EKS、ECS、Fargateのようなコンテナソリューションでは、このようなことが常に起こります。コンテナはノード間で移動され、サービスはスケールアップ/スケールダウンが行われ、コンテナインスタンスが削除されることがあります。問題の根本原因を特定し、その問題が悪意のある活動から来るものなのか、それともアプリケーションの設定ミスなのかを認識できるようにする必要があります。

CloudWatchはログ、メトリクス、イベントを使用してインサイトを提供しますが、それは動的コンテナのトラブルシューティングのために構築されたものではありません。コンテナは刹那的な性質を持っているため、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。侵入者が取った手順をどのように再現するのか？彼らはどのようにアクセスしたのか？どのような影響があったのか？マルウェアはインストールされたのか？データは流出したのか？攻撃はどこまで及んだのか？

Sysdigが追加する機能

SysdigのActivity Auditは、インシデント対応を迅速化し、EKS、ECS、Fargate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、オーケストレータのアクティビティをキャプチャーして関連付けるため、SOCチームは何が起こったのかを特定できます。Sysdigキャプチャーを使用すると、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、すべてのコンテナアクティビティを詳細レベルで記録できるため、チームは、コンテナがなくなった後でもイベントを詳細に理解した上で、Kubernetesフォレンジックを実施できるようになります。



詳しくは、SysdigのActivity Auditを使ったKubernetesでのインシデント対応をご覧ください。

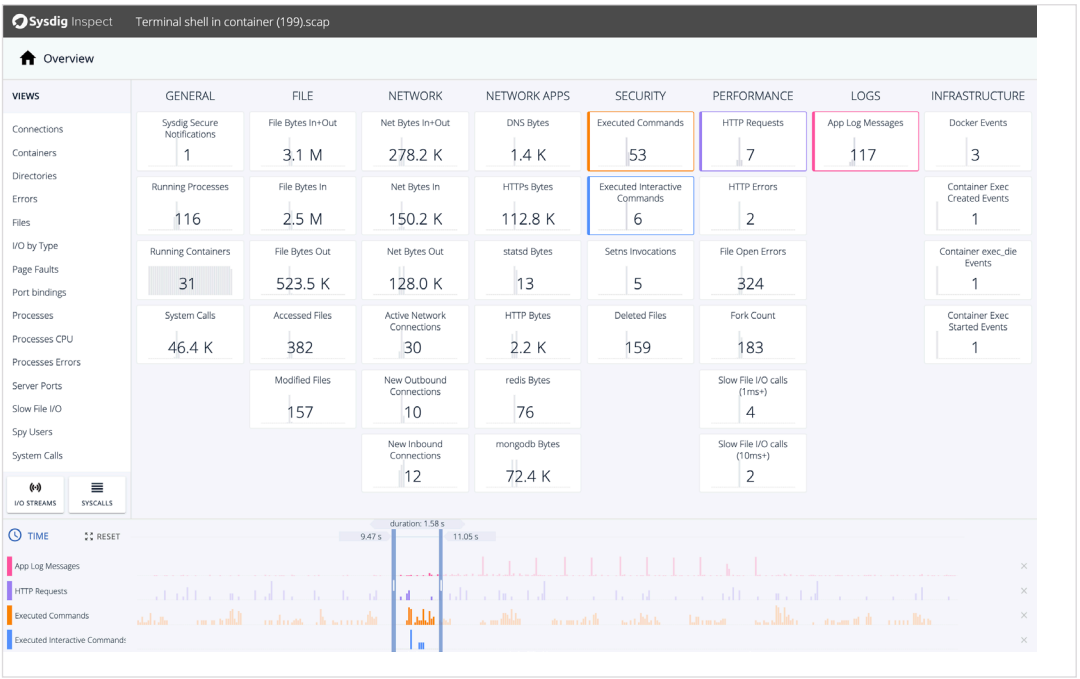
Sysdigは、アラートチャンネル、AWS SNS、またはSIEMに通知を配信します。これにより、コンテナ環境全体のセキュリティに関する知見を集約し、セキュリティアラートを表示管理したり、AWSアカウント全体のコンプライアンスチェックを自動化したりできます。Sysdig SecureとFalcoの両方がFireLensを通じてCloudwatchにイベントを送信することは、EKS & ECS上のFalcoとAWS Firelensによるマルチクラスターセキュリティに見られる通りです。

Sysdigを利用することで、セキュリティチームはPod内の問題を解決し、AWSのコンテキストと関連するシステムアクティビティを再構築することでフォレンジックを実施できます。

Sysdigが提供する機能

- **詳細なフォレンジックレポート**により、セキュリティ侵害の影響を迅速に把握し、封じ込めることができます。

- 詳細なアクティビティ記録により、何が起こったかを迅速に判断する合理的なインシデント対応。監査証跡により、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、イベントなど、侵入時に行われた手順を簡単に再現できます。これにより、データ流出、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、迅速な復旧と今後の防御の強化が可能になります。
- 本番環境外のコンテナに関する**事後分析**。これにより、EKS、ECS、またはFargateコンテナが実行され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できます。



AWSとSysdig Secure DevOps Platformの連携を通じて、より優れた機能を実現

SysdigとAWSは長年のパートナーシップを有しており、両社は提携を通じて、ワークフローを容易に移行し、AWSコンテナやクラウドサービスの上に構築されたアプリケーションに移行できるように支援しています。Sysdigを利用することで、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。すなわち、迅速な開発と提供、継続的な革新、ビジネスとテクノロジーの運用の拡大、資本コストの変動への対応、ユーザー、データ、リソースの保護に必要なセキュリティと可視化などを実現できます。

Sysdig Secureは、AWSの責任共有モデルの一部を維持することを可能にする、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するDevOpsおよびクラウドチームが、ワークフローにセキュリティを組み込み、パフォーマンスと可用性を可視化し、コンテナを監視し、コンプライアンス要件を実装できるようにするものです。

これらの統合はすべて、SysdigがAWS Partner Network（APN）のAWS Advanced Partnerとして、コンテナセキュリティ、モニタリング、DevOpsのコンピテンシーとしてサポートしているものです。我々の目標は、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念頭に置かなければならないセキュリティとモニタリングのレイヤーはいくつかあります。次の表は、これらのレイヤーを要約し、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による共同の利点を取り上げたものです。

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のメリット
Kubernetes	Amazon Elastic Kubernetes Service (EKS)	セキュリティコンプライアンスと監視を自動化し、コンテナ、Kubernetes、クラウドを安心して実行できるようにします。
クラウドコンテナ	AWS Elastic Container Service (ECS)	セキュリティコンプライアンスと監視を自動化し、コンテナ、Kubernetes、クラウドを安心して実行できるようにします。
コンテナのためのサーバーレスコンピュート	AWSファーゲイト	AWS Fargateのセキュリティ体制、脆弱性、脅威、パフォーマンスを包括的に可視化し、統一的なビューを得ることができます。

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のメリット
ホストOS	Amazon Linux 2、Bottlerocket	OSおよび非OSの脆弱性を特定するためのホストスキャンを実施します。EC2の設定を分析し、ホストがCISベンチマークのベストプラクティスに適合していることを確認します。
アクセス制御とクラウドインフラストラクチャーエンタイトルメント管理 (CIEM)	AWS Identity and Access Management (IAM) IAM Access Analyzer	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します。 過剰なパーミッションやエンタイトルメントを可視化し、最小権限でアクセスの管理や強制を行い、アクセス制御の監査を簡素化してコンプライアンスに対応します。 サービスベースのアクセスコントロールを導入し、個々のユーザー/チームに対するセキュリティと情報の監視を合理化します。
イメージスキャニングと脆弱性管理	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）内で、導入前のイメージをスキャンできます。 ランタイム脆弱性レポートを取得し、新しいCVEの影響を評価できます。
コンプライアンス	AWSの構成	CIS、PCI、NIST、SOC 2など、すぐに使える設定チェックで継続的なコンプライアンスを実施し、カスタム評価とダッシュボードでレポートを作成します。
ネットワークセキュリティ	Amazon EC2のセキュリティグループ	Kubernetesのネイティブなネットワークポリシーの使用を自動化および簡素化します。Pod、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します。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実装します。

セキュリティレイヤー	AWSソリューション	Sysdig + AWSのメリット
ファイル整合性監視		Sysdig Secureファイルシステムポリシーでは、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疑わしい変更に対して警告を発行できます。
クラウドワークロード保護 ランタイムの検知と脅威の防止		AWS、ECS、EKSのあらゆるラベル/メタデータに基づく実行時セキュリティポリシーをスコープし、異常な動作を検知して防止します。 システムコール、CloudTrailログ、監査イベントによる深い可視性とAWSメタデータを組み合わせ、攻撃を検知してブロックします。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Falcoを搭載しています。
クラウドセキュリティ体制管理	AWS CloudTrail CIS AWS Foundationベンチマーク AWS GuardDuty	クラウドアセットを発見し、設定の問題を可視化し、クラウドサービスの脅威を検知します。 Sysdigは、CSPMとクラウド脅威検知をクラウドワークロード保護と統合し、AWSクラウドサービスにおける脅威の検知時間を短縮します。
コンテナフォレンジック		ECSやEKSがコンテナやPodを終了した後でも、フォレンジックや事後分析を実施します。

結論

AWSのクラウドとコンテナサービスは、顧客と市場のニーズを満たすソリューションを提供できるようにするために、迅速な移行とイノベーションを支援しています。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のためのカバレッジを提供します。アプリケーション、クラスター、拠点、統合をスケールアウトする際、Sysdigはオープンソースの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を通じて、コンテナ、Kubernetes、クラウドの確実な運用を支援します。Sysdigは、統一されたセキュリティとディープな可視性を通じてAWSサービスを補完します。これらの機能は実行と拡張が根本的にシンプルであり、AWSのパブリックおよびハイブリッドクラウドインフラストラクチャーを使用して運用することを選択した場合、これらを使うことで、あらゆる場所でワークロードを保護できるようになります。

Sysdig Secure DevOps Platformを使うと、あなたの会社のチームが、
クラウドネイティブなアプリケーションを本番環境でいかに自信を持って
運用できるようになるかをご覧いただけます。
プラットフォームに関する詳細や、個別のデモについては、
弊社までお問い合わせください。

Sysdigについての詳細は www.sysdig.jp

Sysdig Japan合同会社
〒107-0052 東京都港区赤坂7-9-4 赤坂Vetoro 3階
https://sysdig.jp/company/contact-us/