sysdig

AWSコンテナサービスにおけるセキュリティと監視

本文の内容は、Security and Monitoring on AWS Container Services account(https://dig.sysdig.com/c/pf-aws-container-security-monitoring-guide?x=u_WFRi&utm_source=gated-organic&utm_medium=website）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コンテナサービスにおけるセキュリティと監視 **5**

AWSユーザーがセキュリティと監視を最重要視する理由 **7**

開発者の方 7

クラウド/DevOps 7

セキュリティとコンプライアンス 8

SysdigでAWSコンテナサービスのセキュリティと監視を管理する **9**

セキュリティの組み込み 9

パフォーマンスと可用性の最大化 9

コンプライアンスの検証 9

AWSコンテナサービスのセキュリティ **13**

ホストのセキュリティ 13

認証と承認 **15**

AWSが提供する... 15

Sysdigが追加したのは... 15

イメージスキャン **16**

AWSが提供する... 16

Sysdigが追加したのは... 16

ファーゲートイメージのローカルスキャン **19**

CI/CDパイプラインのセキュリティ **19**

AWSが提供する... 19

Sysdigが追加したのは... 20

イメージアシュアランス **21**

AWSが提供する... 21

Sysdigが追加したのは... 21

レジストリのセキュリティ **22**

AWSが提供する... 22

Sysdigが追加したのは... 23

コンプライアンス **23**

AWSが提供する... 23

Sysdigが追加したのは... 24

ファイル整合性監視(FIM) **27**

ランタイムセキュリティ **30**

セキュリティ監視 30

Sysdigが追加したのは... 30

脅威の検出 31

AWS CloudTrailのログを利用した脅威の特定 33

ランタイムイメージのプロファイリング 34

Kubernetesネイティブコントロールによる脅威の防止 35

AWSコンテナサービスの監視 **37**

AWSが提供する... 37

Sysdig が追加したのは.... 38

Kubernetesとコンテナの監視 38

アプリケーションとサービスの監視 39

サービスメッシュの可視性 42

AWSが提供する... 42

Sysdigが追加したのは... 42

コンテナフォレンジックとインシデント対応 43

Sysdigが追加したのは... 43

AWSコンテナサービス＋Sysdig Secure DevOps Platformとの連携でより良いものに 46

コンテナプラットフォーム 46

セキュリティ 47

監視／可視化 48

まとめ 49

追加リソース 50

AWSコンテナサービスにおけるセキュリティと監視

企業が初期のサンドボックスから本番環境への移行を始めると、コンテナのセキュリティ、コンプライアンス、信頼性を維持するための運用上の課題に直面します。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プロセスを実装する方法を破壊します。コンテナは、優れた移植性と分離性を提供し、アプリケーションを開発から運用に移行するのに理想的です。しかし、コンテナはブラックボックスのようなものであり、監視とセキュリティを確保するために内部を見ることが難しくなっています。

クラウドチームは、アプリケーションをスケールでより速く提供するために、Amazon ECS、Amazon EKS、AWS FargateなどのAmazon Web Services（AWS）のコンテナサービスを採用するケースが増えています。コンテナやオーケストレーションを用いたアーキテクチャのロールアウトに伴い、アプリケーションやインフラストラクチャのセキュリティ、パフォーマンス、健全性を維持するために必要なものも変化してきています。

Sysdigは、AWSのお客様をサポートするための実績、信頼性、技術的な熟練度を持っています。Sysdig Secure DevOps Platformは、AWSのコンテナサービス上にセキュリティを埋め込み、可用性を最大化し、コンテナライフサイクル全体でコンプライアンスを検証するために企業が求めるスケール、パフォーマンス、ユーザビリティを提供します。

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セキュアなDevopsワークフローを作成することで、組織はデプロイを加速し、Sysdigを使用してAWSコンテナサービス上で本番環境のコンテナワークロードを自信を持って実行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。

- ビルドプロセス中にセキュリティポリシーと設定を検証することでデプロイをスピードアップ
- 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
- インフラストラクチャ、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することで問題を防止
- インシデント対応を加速し、コンプライアンスを合理化するための単一の真実のソースを持つ

AWSコンテナサービス上でのセキュリティと監視のガイドでは、セキュリティ、コンプライアンス、監視をDevOpsワークフローに組み込むことで、クラウドアプリケーションをより速く出荷する方法について説明しています。Sysdig Platform for AWS container servicesは、企業が求めるスケール、パフォーマンス、ユーザビリティを備えたオープンな設計となっています。

AWSユーザーがセキュリティと監視を最重要視する理由

Amazon Elastic Kubernetes Service (EKS)とElastic Container Service (ECS)はフルマネージドのコンテナオーケストレーションサービスです。これらは、開発、運用、セキュリティチームがコンテナ化されたワークロードを構築、デプロイ、安全に実行し、コンテナアプリケーションのデプロイを高速化するための素晴らしい体験を提供するように設計されています。

AWSでのコンテナのデプロイには、さまざまなオプションが用意されています。AWSでコンテナをデプロイするには、ECS、kopsやkubeadmを使ってEC2の上にKubernetesをセットアップする方法、Amazonが提供するフルマネージドのKubernetesサービスであるEKSを利用する方法があります。ECSやEKSと並んで、AWS Fargateというサーバーレスコンピュートエンジンをコンテナに利用することもできます。

しかし、チームや役割によって、可視性やセキュリティ、本番環境に移行するためにはどのようなプロセスが必要なのかなど、懸念事項や視点が異なります。

開発者の方

AWSのコンテナサービスは、開発者が基礎となるインフラストラクチャーの詳細を知らなくても、コンテナ化されたアプリケーションやオーケストレーションを活用できるようにします。AWSの継続的インテグレーションと継続的デリバリ（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、デプロイのプロセスを合理化します。AWS CodeBuildやAWS CodePipelineなどのAWSフレームワークを使ってソースコードとベースイメージを組み合わせることで、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の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。これらのイメージに既知の脆弱性がないことを保証し、セキュリティのベストプラクティスに従うことは、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くする大きな課題です。

クラウド/DevOps

DevOpsチームは、アプリケーションや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、パフォーマンスの維持を担当します。ユーザーは内蔵のAWSウェブコンソールを利用してインフラストラクチャーとプラットフォームの機能を管理し、プレイブックを利用してアプリケーションのデプロイを自動化します。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使って、プラットフォームにセキュリティを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、異常な動作やゼロデイ攻撃から守るために、AWSのコンテナ環境を実行時に継続的に監視し、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。チームは、新しいコンテナインフラストラクチャーとデプロイされたアプリケーションが、規制や内部コンプライアンスの要件に適合していることを確認するために監視する必要があります。

SysdigでAWSコンテナサービスのセキュリティと監視を管理する

セキュリティ、コンプライアンス、モニタリングを統合することで、企業はプライベート環境、ハイブリッド環境、マルチクラウド環境において、AWSコンテナサービス上でクラウドネイティブのワークロードを自信を持って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を最大化し、セキュリティリスクを管理し、クラウドアプリケーションをより迅速に出荷することができます。

AWSのコンテナサービスは、コンテナプラットフォーム全体のセキュリティと監視をベースラインでカバーしています。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ーの数を増やしていくと、SysdigはAWSコンテナサービスを拡張し、以下のようなセキュリティと監視機能を提供します。

セキュリティの組み込み

- AWSコンテナサービス、および複数のプロバイダーにまたがるその他のコンテナおよびクラウドワークロードのセキュリティ監視
- サードパーティライブラリ、構成検証、脆弱性管理を含む広範なイメージスキャン
- ランタイムセキュリティによる攻撃の検出と防止、ゼロデイ脅威対策の実施
- インシデント対応、コンテナのフォレンジック、コンテナアクティビティの詳細な可視性を備えた監査

パフォーマンスと可用性の最大化

- AWSコンテナインフラストラクチャー、サービス、アプリケーションのフルスタック可視化により、パフォーマンスと健全性を監視し、問題を防止します
- クラウドスケールでのクラスタ間のPrometheusモニタリングの拡張 - 粒度の細かいシステムコールデータに基づいた単一の情報源によるトラブルシューティングの迅速化

コンプライアンスの検証

- アプリケーションのライフサイクル全体にわたってコンプライアンスを継続的に検証し、NIST、PCIなどの規制コンプライアンス基準の実装を支援します
- CIS ベンチマークおよび内部セキュリティ標準に対する構成をチェックします
- Kubernetes、コンテナ、クラウドのアクティビティを関連付けることで、監査を加速します

Sysdig Secure DevOps Platformは、唯一の統一されたコンテナセキュリティおよび監視プラットフォームです。Sysdigは、単一の真実のソースで、開発、DevOps、セキュリティチーム間の情報のサイロを排除します。この統合データプラットフォームにより、DevOpsチームはインシデントを正確にトリアージし、インシデントの原因が設定ミスや悪意のある試みによるものかどうかを迅速に判断し、コンテナがなくなった後もフォレンジックを実行することができます。

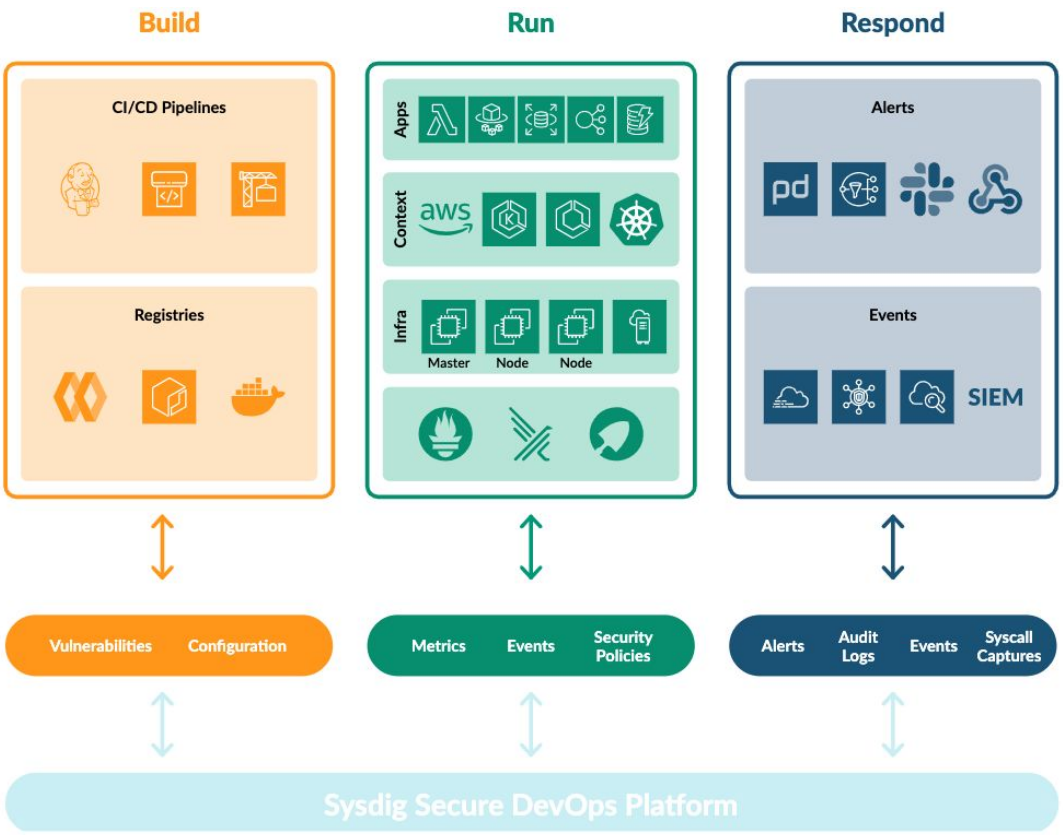
DevOps チームは、特定のネームスペースやクラスター内の実行イメージに影響を与える脆弱性をレポートすることができます。例えば、新しいCVEが登場した場合、Sysdig Secure DevOpsプラットフォームは、特定のパブリッククラウド(AWS)のリージョン、ネームスペース、クラスターなどで影響を受けたイメージと、その修正プログラムを所有しているチームをDevOpsチームが迅速に特定できるようにします。このアプローチにより、組織は脆弱性や粒度の細かいシステムデータをクラウドやKubernetesのコンテキストに自動的に相関させて分析することで、問題を迅速に解決することができます。

Sysdigは、信頼性と安全性の高いクラウドアプリケーションの提供を支援し、AWSのコンテナサービスを大規模に運用するための一元化された可視性とセキュリティを提供します。Sysdigは、AWSでホストされた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は10,000以上のノードにスケールし、AWSコンテナサービスのクラスタ上で稼働しているコンテナやアプリケーションをセキュアに監視することができます。

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、キュレーションされたワークフローにより、すぐに開始することができます。Sysdigは自動化とすぐに使える統合機能を使用して既存のDevOpsワークフローにプラグインしているため、可視性とセキュリティ管理が遅くなることはありません。

以下に示すように、SysdigはアプリケーションのライフサイクルAWSのコンテナサービスプラットフォームを強化します。これにより、お客様はAWSコンテナサービスプラットフォーム

にさらなる信頼を得ることができ、ビジネスはデジタルトランスフォーメーションの取り組みを加速し、拡大することができます。

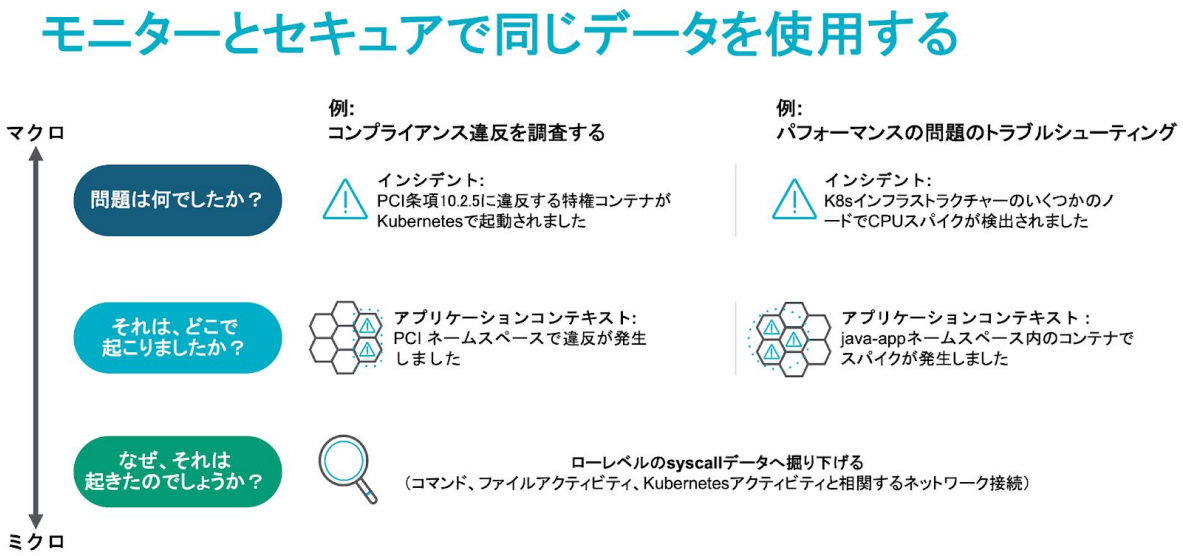


また、Sysdigは以下の機能を利用してAWSコンテナサービスのコンテナとオーケストレーションのインサイトを提供しています。

- ImageVision™は、脆弱性や設定ミスのあるイメージを識別し、デプロイされないようにします
- ContainerVision™は、コンテナ内やマイクロサービス全体でリクエストレベルの可視性を提供します。侵襲的な計測を行わずに、詳細なメトリクスとイベントを提供します。
- ServiceVision™はECSとEKSと統合して、オーケストレーションのメタデータですべてのメトリクスとイベントを自動的に豊かにします。

要するに、これらのテクノロジーは、パイプラインやクラスターのどこにセキュリティやパフォーマンスの問題があり、注意が必要なのかをピンポイントで特定するのに役立ちます。ネームスペース、

デプロイメント、ポッドなどのKubernetes論理リソースを介して情報を可視化してセグメント化する機能により、どのサービスがどこに影響を受けているかを正確に把握することができます。



AWSコンテナサービスのセキュリティ

ここでは、AWSが提供する様々なセキュリティコントロールと、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全体で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してい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
- Amazon ECR.Clair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

ホストのセキュリティ

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上でコンテナを安全に運用するために、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安全で安定した高性能な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。それは、潜在的なセキュリティ脆弱性への暴露を制限し、非重要なパッケージの数を削減します。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期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のオペレーティングシステムで、AWSが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開発したものです。Bottlerocketにはコンテナを実行するために必要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

リティ攻撃の対象となる領域が減少し、管理のオーバーヘッドが軽減されます。Bottlerocketでは、セキュリティアップデートが提供されるとすぐに自動的に適用され、障害が発生してもロールバックすることができるため、混乱を最小限に抑えることができます。

これらのソリューションは、クラウドでのセキュアな運用を可能にするだけでなく、AWS Outpostsを利用したオンプレミスの仕組みでも活用することができます。Sysdigは、パブリック、プライベート、ハイブリッドのデプロイメントにおいて、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、お客様はAmazon EKSとECSを使用してこれらのソリューションを使用して、本番環境でコンテナワークロードを安全かつ一貫して実行できるようになります。

認証と承認

AWSコンテナサービスへのユーザーアクセスは、Web UI、CLI、APIなどの標準インターフェースを介して提供されます。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制御および測定しますか？

AWSが提供する...

AWS Identity and Access Management（IAM）を使用すると、AWSサービスと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できます。 IAM管理者は、Amazon EKSおよびECSリソースを使用するための認証（サインイン）および承認（権限を持つ）できるユーザーを制御します。

Sysdigが追加したのは...

Sysdigを使用すると、AWSコンテナサービスの可視性、メトリクス、通知、セキュリティポリシーにアクセスできるユーザーを定義できます。これはチームと呼ばれ、既存のAWS IAMメカニズムを補完するサービスとメタデータベースのアクセス制御の概念を導入します。Sysdigチームを使用すると、管理者はAWSにデプロイされた限定されたサービスまたはサービスのセットにアクセスできるユーザーのグループを定義できます。たとえば、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表示する場合があります。アクセス制御による公開を制限し、特定のチームごとにデフォルト構成を提供することで、ユーザーとチームのセキュリティ情報を合理化できます。Sysdigは、ロールベースのアクセス制御（RBAC）をサポートしてユーザー特権を定義し、組織内のさまざまなチーム間でフェデレーションアクセス制御を提供します。管理者の役割に加えて、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のさまざまなアクセス役割を利用できます。

イメージスキャン

アプリケーションとインフラストラクチャーコンポーネントは、すぐに利用できるパッケージの上に構築されており、その多くは、古いライブラリバージョンを含む可能性のあるオープンソースソフトウェアです。これらのパッケージが最初にどこから来たのか、誰が作成したのか、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が重要です。

AWSが提供する...

Amazon Elastic Container Registry（ECR）は、開発者がDockerコンテナーイメージを簡単に保存、管理、デプロイできるようにする、フルマネージドのDockerコンテナーレジストリです。 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、開発から本番ワークフローまでを簡素化します。

AWSでのコンテナ導入が本格化する中、ECRの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第一歩となります。ECRは、オープンソースのClairプロジェクトのCommon Vulnerabilities and Exposures (CVE)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ています。ECRから引き出されたイメージを脆弱性と設定ミスの両方をスキャンして、悪用可能なAWS上で動作するアプリケーションをプッシュしないようにする必要があります。

Sysdigが追加したのは...

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組み込んでいます。15以上のCVE脅威フィードを活用し、Sysdig Secureは単一のワークフローで脆弱性とセキュリティやコンプライアンスに関連した設定ミスを検出します。チームがアプリケーションを構築する際に、Sysdigは脆弱性のあるイメージがCI/CDパイプライン（Jenkins、Bamboo、GitLab、AWS CodePipelineなど）を介してプッシュされるのを防ぎ、本番環境での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超える追加のECRスキャン機能を提供します。ECRで設定すると、Sysdig Secureはレジストリ内に保存されているすべてのイメージをエンジンに取り込み、解析を行います。チームは、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からのPythonパッケージやJava JARファイルなどのサードパーティライブラリから検出することができ、開発者が本番前にアプリケーションイメージに引き込んでいる可能性があります。

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

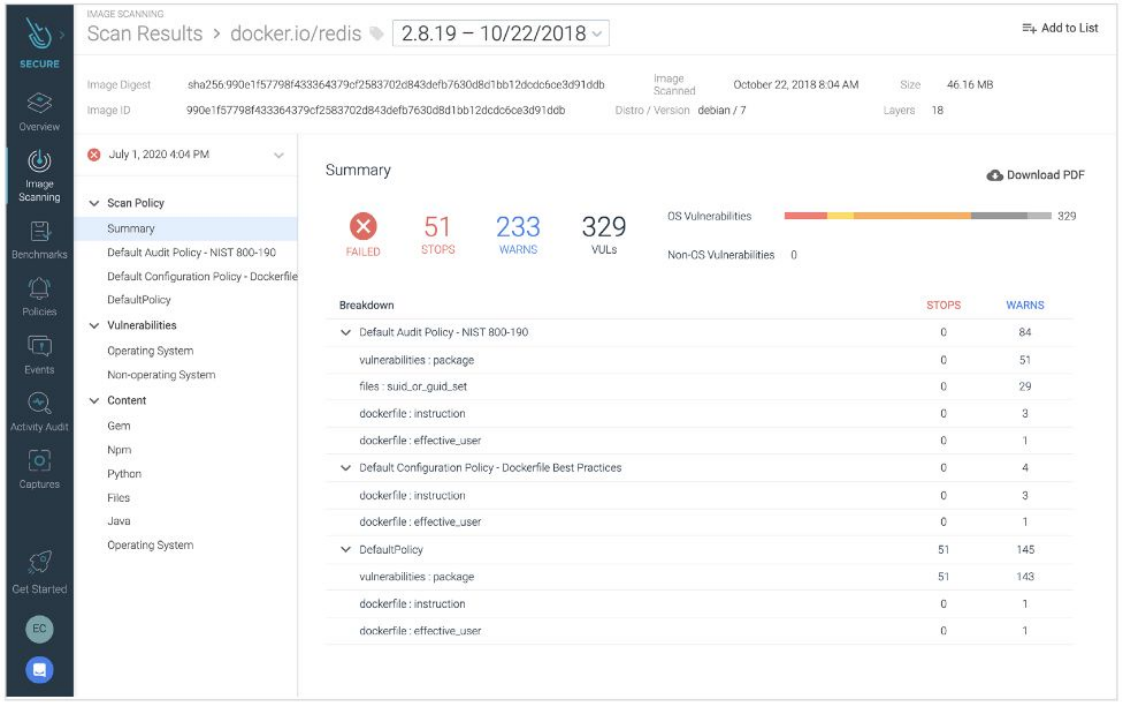
- 標準的なアプローチでは、スキャンのためにSysdigにイメージを送信する必要があります。スキャン後、Sysdig Secure UI内で結果を確認することができます。
- インライン スキャンとも呼ばれるローカル スキャンは、CI/CD パイプラインまたは ECR レジストリ内で直接イメージをスキャンします。このオプションを使用することで、レジストリの認証情報やイメージの内容をAWS環境外で共有する必要がないため、より安全なアプローチが可能になります。また、スキャンを自動化し、ECR内で直接レポートを生成することで、スキャン結果を迅速に得ることができます。

Sysdig Secureは以下のような可視性を提供します。

- 公式のOSパッケージの脆弱性
- 非公式パッケージの脆弱性
- 設定チェック (例: Dockerfile で SSH を公開している場合、root として実行しているユーザ)。
- 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ライブラリの脆弱性。
- 秘密、トークンや証明書などのクレデンシャル、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対して評価されます。Sysdig Secure スキャンポリシーは、イメージ内の脆弱

性、設定ミス、またはコンプライアンスの問題を検出し、UIで直接合否結果を生成するのに役立ちます。



ファーゲートイメージのローカルスキャン

Fargateユーザーにとって、Sysdigに固有の機能は、開始時にFCR内のイメージのスキャンをトリガーしてECRタスクを実行する機能です。Amazon EventBridgeを利用して、SysdigはFargate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配信プロセスのステップを自動化することで、チームがより速く、より頻繁に顧客にアップデートを配信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うことができ、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...

AWSでは、継続的インテグレーション/継続的デリバリパイプラインを設定して、ソフトウェアのデリバリプロセスを自動化することができます。

AWSでは、DevOpsチームがソフトウェアのデリバリプロセスを自動化するためのツールがいくつか提供されています。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、コードの自動デプロイのためのCodeDeployである。これらのツールに加えて、CodePipelineを利用することで、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は完全に管理された継続的インテグレーションサービスで、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作成する。CodeBuildは継続的にスケーリングし、複数のビルドを同時に処理するため、ビルドが待ち行列になってしまうことはありません。

AWS CodePipelineは、アプリケーションやインフラのアップデートのためのリリースパイプラインを自動化する、完全に管理された継続的な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、デプロイのフェーズを自動化します。

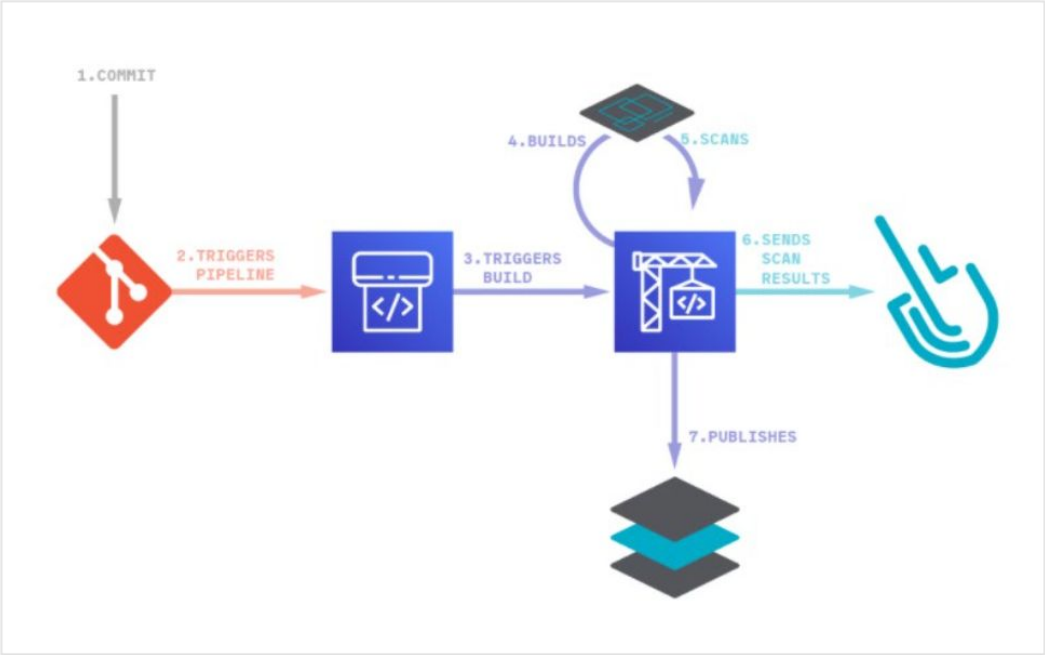
Sysdigが追加したのは...

AWS CodeBuildとCodePipelineのイメージスキャンは、既知の脆弱性を検出し、パイプラインの早い段階でコンテナのビルド構成を検証することで、DevOpsチームのデプロイメントのセキュリティに対する信頼性を高めます。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る前にこれらの問題を検出することで、修正をより迅速に適用し、本番環境への配信時間を向上させることができます。

Sysdig Secureイメージスキャンは、AWS CodeBuild、AWS CodePipeline、Jenkins、Bamboo、GitLab、CircleCIなど、お使いのCI/CDパイプラインに直接統合されます。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、クレデンシャルの暴露、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用することで、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することができます。

SysdigのスキャンとCI/CDパイプラインの統合を活用することで、開発者はCI/CD UIから離れることなく、障害が発生した理由や修正すべき点を直接理解することができます。非クリティカルな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が示唆してくれます。

Sysdigを使用することで、AWS CodePipelineで構築されたイメージは、インフラストラクチャーを離れることなく、ステージングレジストリを必要とせずにスキャンすることができます。複数のスキャンを並行して実行することができ、スループットを向上させることができます。



イメージアシュアランス

イメージアシュアランスは、コンテナ環境に未承認のイメージがデプロイされないようにすることに重点を置いています。これにより、本番環境で実行する前に定義したポリシーに基づいてイメージを評価・検証することで、問題やエラーを削減することができます。

AWSが提供する...

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に未承認の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の機能を使用して、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していないリクエストを拒否します。

Sysdigが追加したのは...

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する場合、このセキュリティ検

証の決定はAPIに伝搬され、元の要求者に返信し、イメージがチェックをパスした場合にのみ、オブジェクトをetcdデータベースに永続化します。

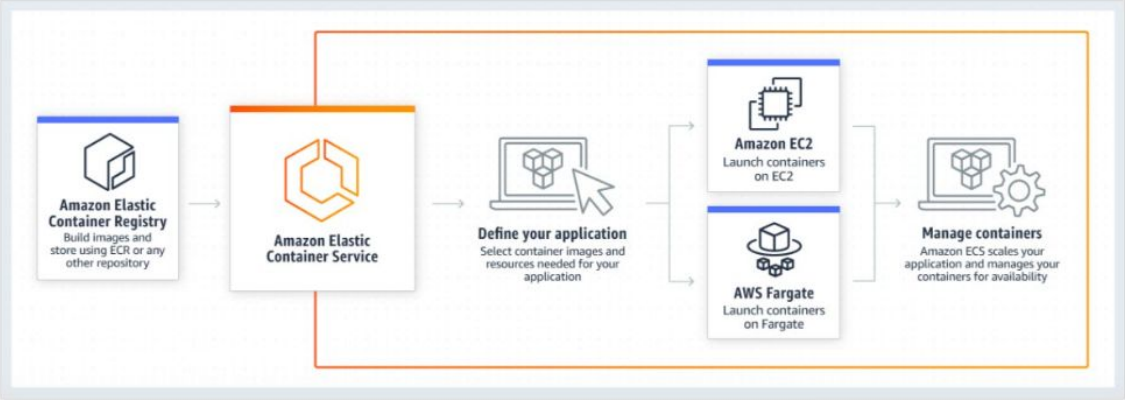
レジストリのセキュリティ

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軽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のプルやプッシュを誰ができるかを管理したり、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に取ることができるステップの一部です。

AWSが提供する...

Amazon ECRは、安全性、拡張性、信頼性に優れたマネージドAWSのDockerレジストリサービスです。Amazon ECRは、AWS IAMを使用して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るようになっています。開発者はDocker CLIを使用してイメージのプッシュ、プル、管理を行うことができます。

AWSコンテナサービスチームはGitHub上で公開ロードマップを管理しています。このロードマップには、各チームが取り組んでいることについての情報が含まれており、すべてのAWSの顧客が直接フィードバックを行うことができるようになっています。詳細については、AWS Containers Roadmapを参照してください。



Sysdigが追加したのは...

Sysdig Secureコンテナイメージスキャンは、CoreOS Quay、Amazon ECR、DockerHub Private Registries、Google Container Registry、JFrog Artifactory、Microsoft ACR、SuSE Portus、VMware Harborを含む、すべてのDocker v2互換レジストリをサポートします。

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、何百、何千ものアプリケーションやサービスが相互に接続されており、多くのユーザが利用しています。このような広大な環境のセキュリティを制御し続けるためには、セキュリティポリシーに準拠しているかどうかをシステムをスキャンする標準的な方法が必要となります。

AWSが提供する...

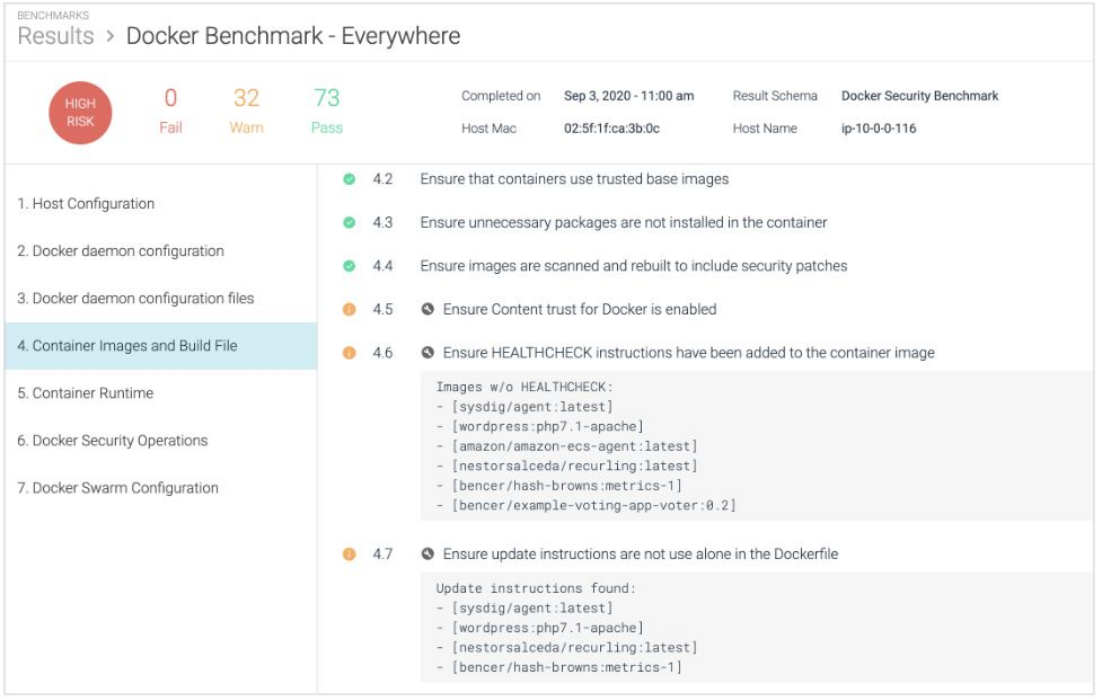
AWS Configは、AWSリソースの構成を評価、監査、評価できるサービスです。AWSリソースの構成を継続的に監視・記録し、記録された構成と希望する構成との比較評価を自動化することができます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化することができます。

Sysdigが追加したのは...

Sysdigは、NISTやPCIなどの規格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。デプロイメントが希望する構成に準拠していることを検証できることは、コンプライアンスの最初のステップの1つです。しかし、コンプライアンスの要件はそれだけでは終わりません。コンテナのコンプライアンスには独自の要件があり、さまざまなポイントで実施する必要があります。

- DockerとKubernetesのCISベンチマークを使用して、コンテナと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をチェックする。
- 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する。
- 実行時には、ポリシーを使用して、MITRE ATT&CKのような攻撃フレームワークを継続的に検出したり、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。
- 最後に、SOC2、PCI、ISO、HIPAAの要件の一部であるコンテナ環境の変更を監査します。

Sysdigはインフラストラクチャー層から始まり、KubernetesベンチマークやDocker CISベンチマークのような特定のホスト、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実行します。また、Sysdigはポリシー違反を修正するための修復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際に、より迅速に解決することができます。



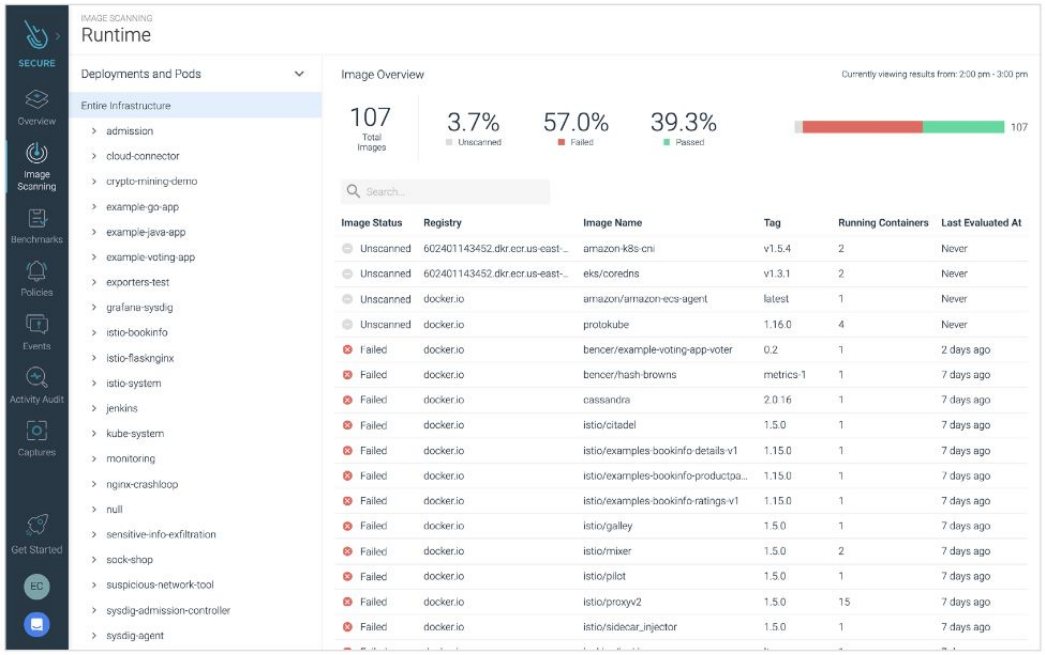
Sysdig Secure は、NIST SP 800-190、PCI DSS、Dockerfile などのコンテナイメージセキュリティとコンプライアンスのベストプラクティスを実装するためのツールを提供します。Sysdig Secureコンテナイメージスキャンポリシーを使用することで、クラウドのコンプライアンスを検証し、イメージレベルで以下のようなベストプラクティスを実施することができます。

- 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を使用し、必要なパッケージのみを使用することを保証します。

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基準を最新のセキュリティポリシーに変換することで、ランタイムコンプライアンスを保証します。これにより、デプロイ後のコンテナの挙動を分析し、ランタイムドリフトを監査することができます。Sysdigは、システム上で実行されたコマンド（ホストでもコンテナ

内でも、docker execやoc attachなど）やKubernetes APIを監査目的でタップします（秘密のリソースへのアクセス、不正ユーザーによるリクエストなどを監査します）。

新たにクリティカル/重要度の高いCVEが公開された場合、Sysdig Secureを使用することで、すぐにエクスポージャーを評価することができます。影響を受けるサービスと説明責任のあるチームを迅速に特定することができます。開発者やアプリケーションの所有者は、Kubernetesを使用して、またはサービス、デプロイメント、アプリケーションなどのクラウドのメタデータを介して特定され、そのイメージや脆弱性を表示するためにアラートが表示されます。

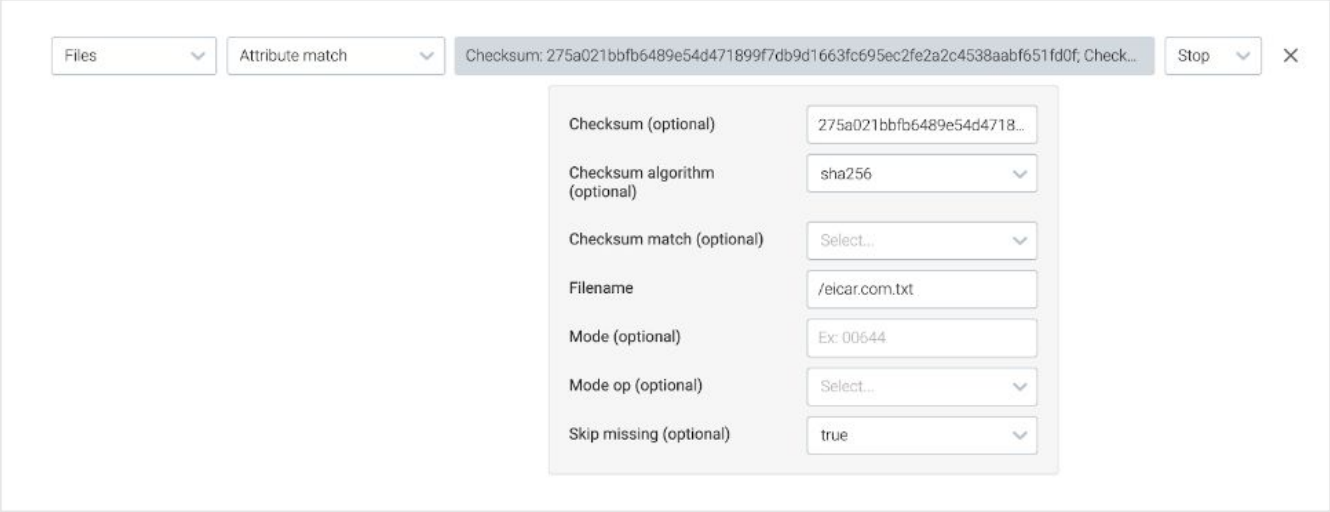


ファイル整合性監視(FIM)

ファイル整合性モニタリングにより、機密ファイル関連のアクティビティのすべてを可視化することができます。活動が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、重要なシステムファイル、ディレクトリ、不正な変更の改ざんを検出するために使用されます。

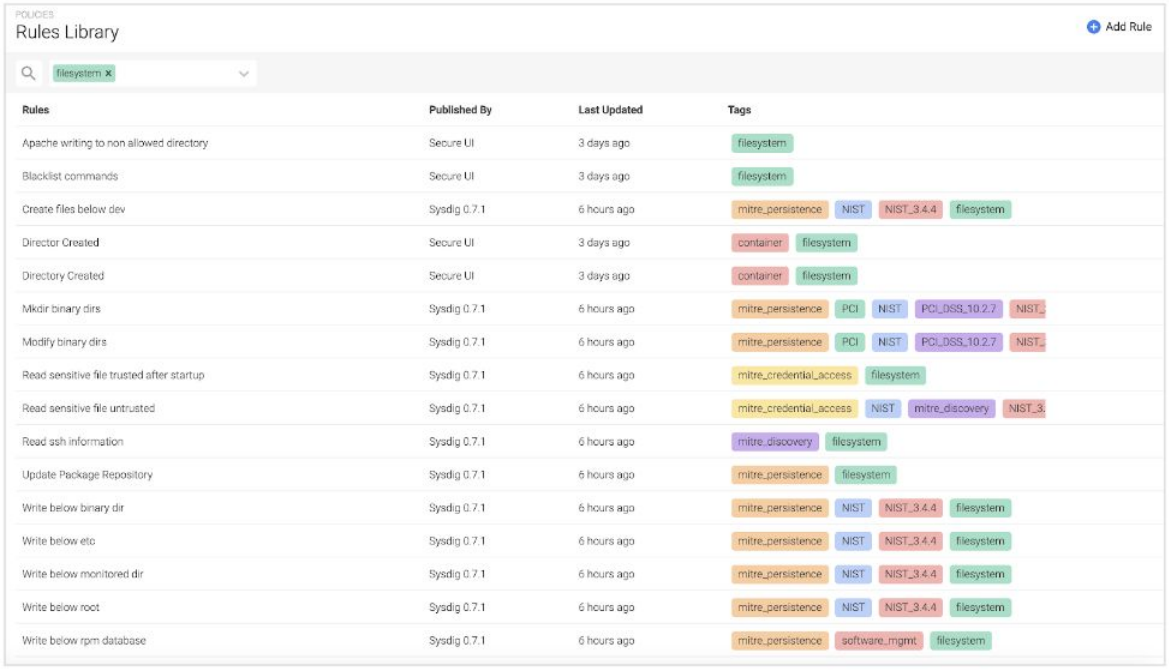
Sysdig Secureを使用すると、特定のファイル属性をスキャンし、CI/CDパイプライン内のイメージスキャンポリシーの一部として埋め込むことができます。これにより、FIMポリシーが満たされていない場合、ビルドを早期に失敗させることができます。ファイル整合性モニタリングポリシーでは、以下のことが可能です。

- ファイルが存在するか不足しているかをチェックし、条件に基づいてアラートをトリガーします。
- SHA256 ハッシュに対して特定のファイルを検証する。特定のファイルを SHA256 ハッシュに対して検証します。コンテナ内のバイナリまたはバイナリの SHA256 はすでに知っています。実行ファイルへの変更は疑わしいものであり、潜在的に危険です。
- 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実行ビットがある場合は、アラートとしてフラグを立てる必要があります。
- 正規表現に基づくファイル名をチェックします。
- 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などがないかどうかを確認する。



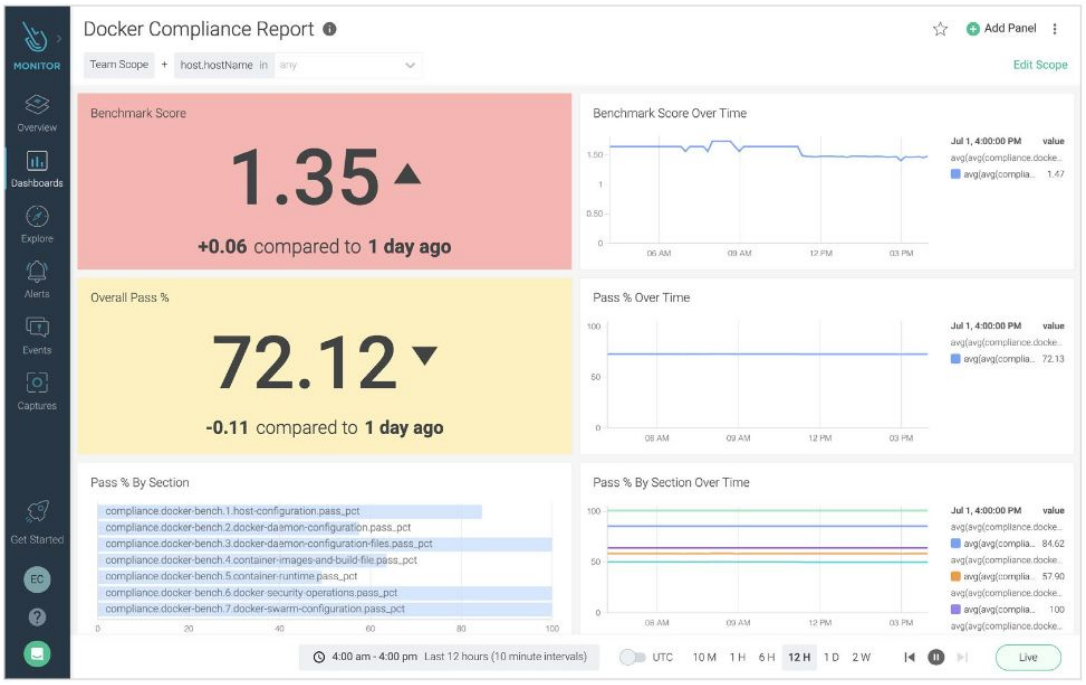
また、ファイルシステムへの不審な変更を警告する FIM ポリシーを実行時に実装することもできます。これらは一般的なファイル整合性監視チェックであり、強固なセキュリティ態勢を強化するためのルールとして含める必要があります。

- - ファイルまたはディレクトリの作成または削除。
- ファイルやディレクトリの名前の変更
- パーミッション、所有権、継承などの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への変更。
- コンテナのパス以下のファイルの変更。
- bash の履歴の削除。



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セキュリティメトリクスとダッシュボードのセットに変換します。社内外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姿勢を分析し、パターンや傾向を迅速に可視化し、コンプライアンス姿勢についての貴重な洞察を得ることができます。

- セキュリティ態勢を過去の時点と比較する。
- 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姿勢を理解する。
- コンプライアンスチェックが受け入れられているポリシーを下回った場合に警告を発する
- AWSコンテナクラスタ全体の構成のドリフトを検出します。



ランタイムセキュリティ

セキュリティ監視

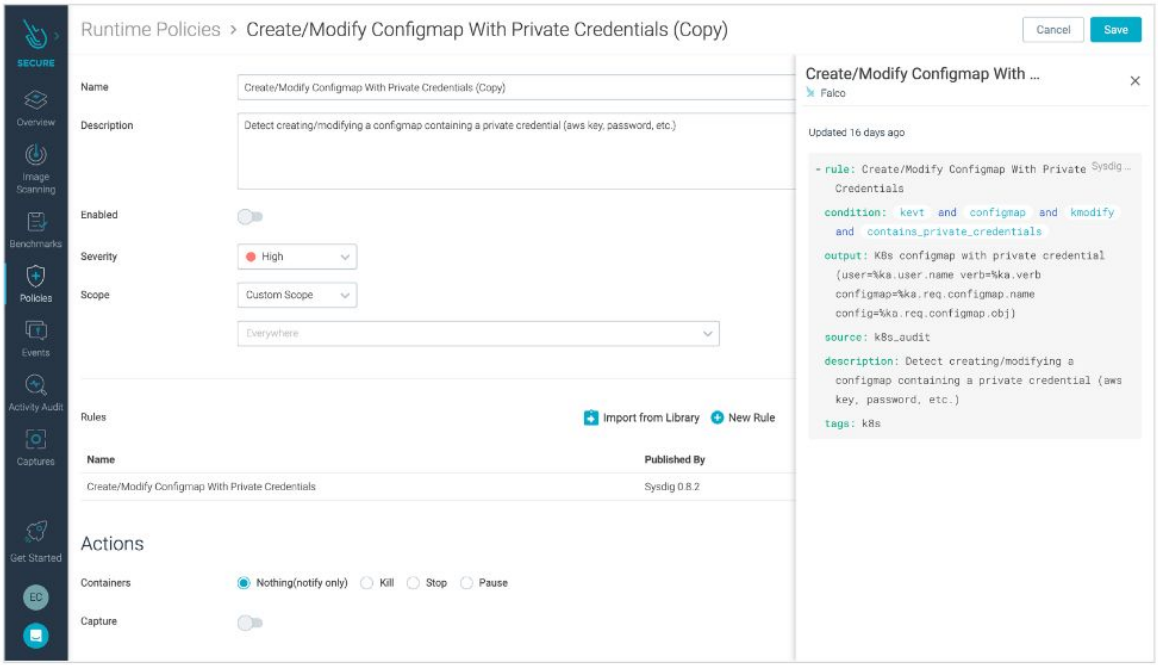
AWSコンテナサービスの監視とセキュリティの両方の可視性を得ることは、トランスフォーメーションを成功させるために必要です。例えば、セキュリティチームは、クリプトマイニングやDoS攻撃が特定のパフォーマンスメトリクスの異常な逸脱によってさらに説明できるかどうかを知る必要があります。

さらに、本番環境に入ったら、最小限の権限とアクセス権限でアプリケーションを構成することでリスクを軽減することが重要です。同時に、ワークロードの動作を観察し、異常なアクティビティを探し、CI/CDやレジストリスキャンで検出され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し、維持する必要があります。

Sysdigが追加したのは...

脅威の検出

Sysdigはオープンソースの検出エンジンであるCNCF Falcoプロジェクトを利用して、実行時にホストやコンテナ上の異常なアクティビティを監視します。また、KubernetesやEKS管理サービスを使用している場合、AWS CloudTrailのログや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インジェストして監視します。



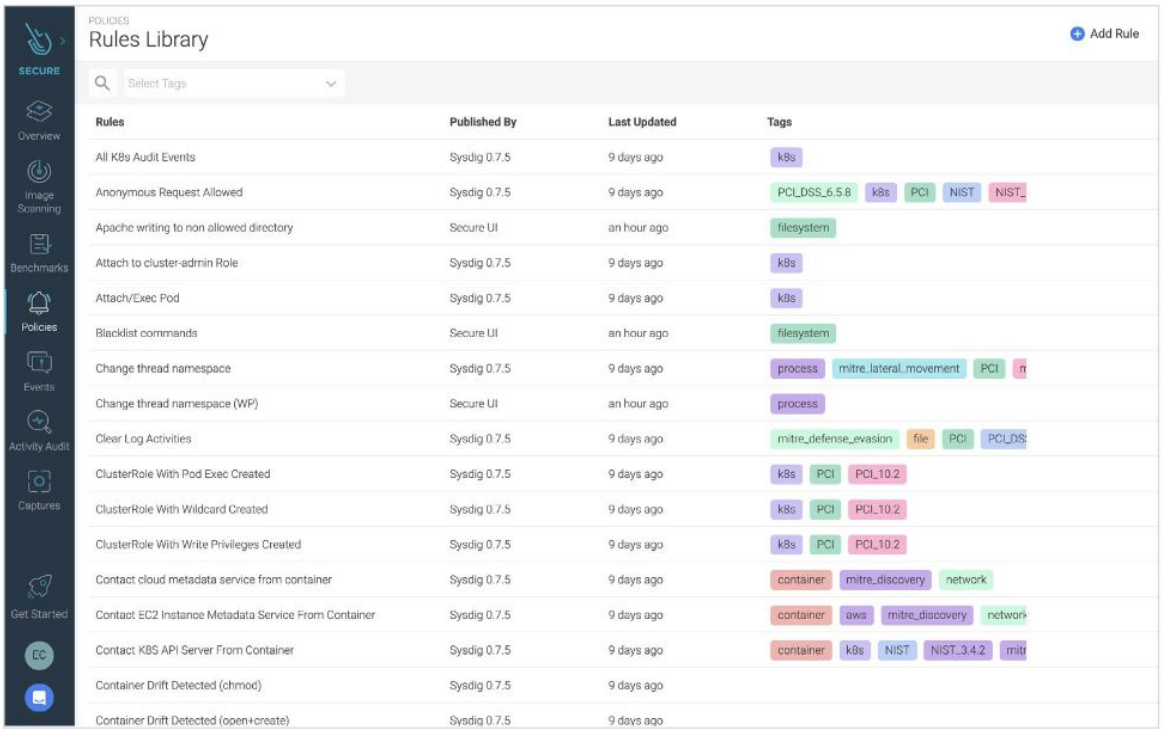
EKSからのKubernetesサーバAPIイベントのインジェストについては[こちら]をご覧ください。

CI/CDプロセスやAWS Elastic Container Registryからコンテナを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、実行時にしか顕在化しません。

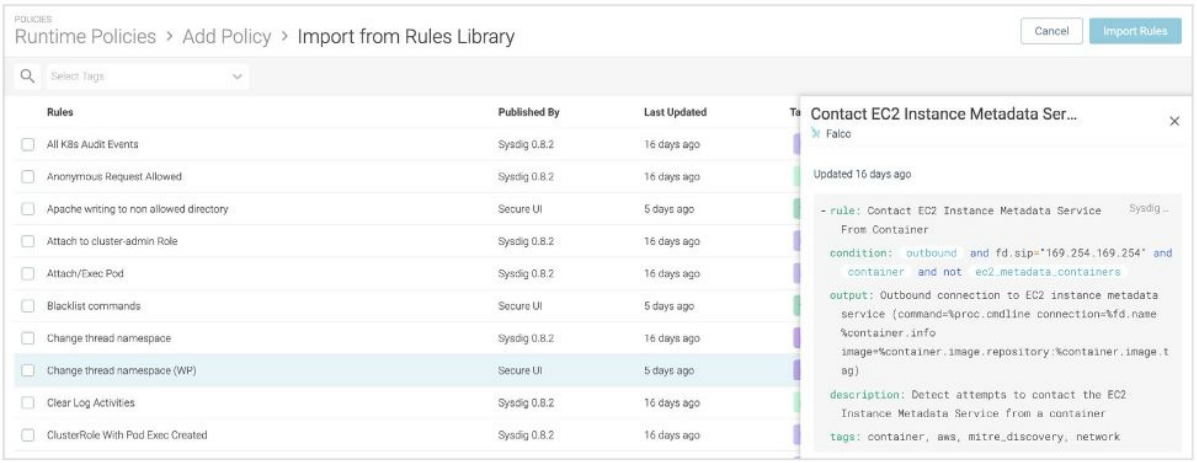
- ゼロデイ脆弱性や、自社のソフトウェアに特有の非公開の脆弱性。
- 不安定な動作やリソース漏洩を引き起こすソフトウェアバグ。
- 内部特権のエスカレーションの試みや、隠れた/埋め込まれたマルウェア。

60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、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することができます。これには以下が含まれます。

- 規制コンテナの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。
- 最も普及しているコンテナ攻撃のランタイム検出：クリプトマイニング、秘密の流出、コンテナ隔離侵害、およびラテラルムーブメントへの移動。
- 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、要件に合わせて細かく調整されたポリシーを構築することができます。コミュニティから提供され、キュレーションされたFalcoルールは、Cloud Native Security Hubで利用可能です。



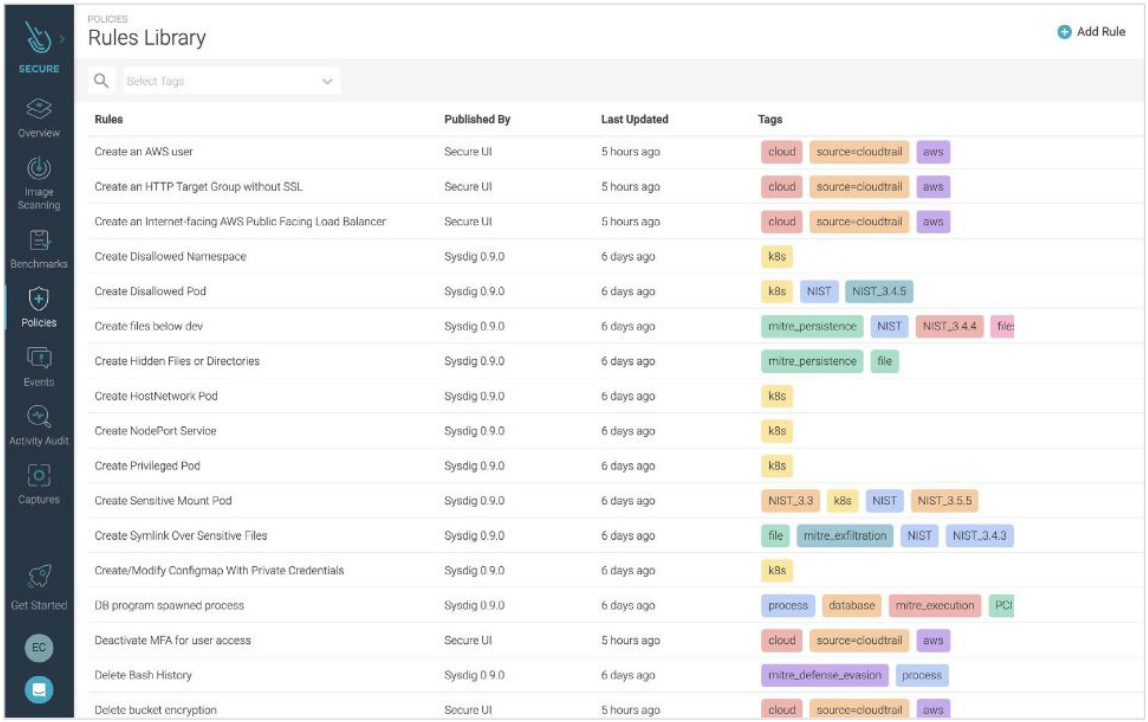
ランタイムルールは、特定のAWSコンテナサービスのクラスタ、ネームスペース、デプロイメント、ポッドなど、任意のスコープに適用することができ、複数のクラスタ、クラウドリージョン、データセンターにまたがるスケールで管理することができます。

AWS CloudTrailのログを利用した脅威の特定

Sysdig Secureは、オープンソースのFalcoランタイムルールを使用してAWS CloudTrailのログを分析することで、AWSサービスへの不正アクセスや設定変更を監視することができます。予め設定されたポリシーを使用したり、独自の検出機能を作成して、予期せぬ活動を警告することができます。

Sysdigを使用することで、以下のような異常な動作を検知することができます。

- IAMポリシーの変更に伴う異常なアクセス権
- 公開されたアカウントやサービス
- 不正アクセス



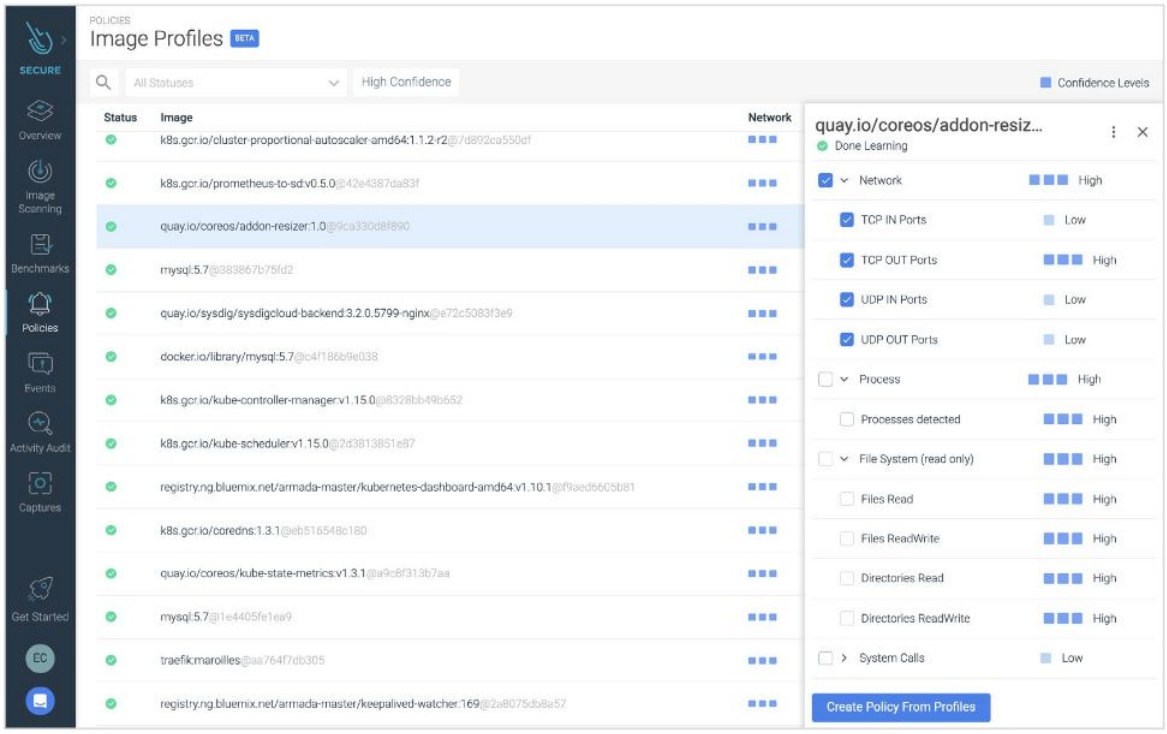
AWSのユーザーやサービスがAPIコールを実行すると、このアクティビティはCloudWatchによって記録されます。Sysdigはこのデータを使用して、IAM、RDS、EC2、RedShift、VPCなどのAWSサービス全体のリスクを分析します。この統合を使用することで、ユーザーは100以上のコミュニティ主導のアウトオブボックスルールを活用して時間を節約することができます。さらに、DevOpsやセキュリティチームは、AWS環境を離れることなく、AWS Security Hubで直接イベントを確認することで、迅速に発見を得ることができます。

CloudTrailがサポートしているサービスのリストは、AWSのWebサイトで確認できます。

ランタイムイメージのプロファイリング

大規模環境でのランタイムセキュリティの作成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を機能させています。イメージプロファイリングは、コンテナのランタイム動作を自動的にモデル化、分析、学習し、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様々なメタデータ

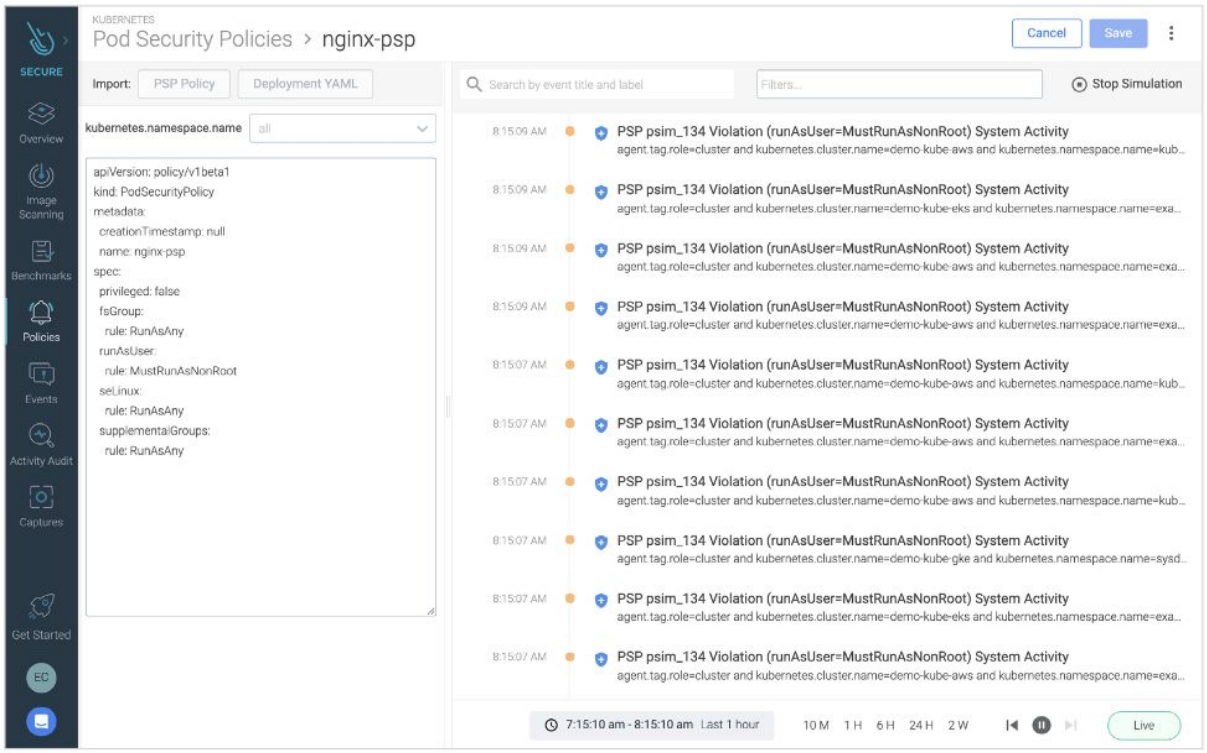
でリッチ化しながら、kube-apiserverのアクティビティやsyscallsを分析することが含まれています。このアプローチにより、機械学習による異常検知が強化され、脅威が伝播する前にブロックできるようになります。



Kubernetesネイティブコントロールによる脅威の防止

Sysdigは、Pod Security Policies (PSP)などのKubernetesネイティブコントロールを使用して脅威を防ぎます。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、適用時にアプリケーションを壊さないようにします。これにより、ユーザーは本番環境でPSPを迅速かつ容易に導入することができます。また、PSPは、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Kubernetesネイティブの制御メカニズムを提供します。

Sysdig Secure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。詳細については、Sysdigの[Kubernetes Policy Advisorを使用した本番環境でのPod Security Policies]のブログで、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]でご紹介しています。



Sysdig Secureを使用することで、運用チームとセキュリティチームはコンテナセキュリティポリシー作成の負担を軽減し、より透明性と保証を得ることができます。

AWSコンテナサービスの監視

コンテナは短命であり、動的であり、常に変化し続けています。コンテナが死んでしまえば、中のものはすべて消えてしまいます。SSHを使ったりログを見たりすることはできませんし、モノリシックアプリケーションに使用されている伝統的な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、一貫してどこにでもデプロイできるので、運用には最適ですが、同時に、トラブルシューティングが難しい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を実現するために非常に重要です。コンテナ上で実行されるマイクロサービス・アーキテクチャにより、アプリケーションの拡張が容易になり、開発期間が短縮されたことで、より迅速なイノベーションが可能になり、新機能の市場投入までの時間が短縮されました。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のインフラストラクチャー上を移動することができます。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ための鍵となります。

AWSが提供する...

AWSはAmazon CloudWatchというサービスを提供しており、ログやメトリクス、イベントを通じてAWSのリソースやアプリケーションの運用状態の健全性を監視・観察することができます。

CloudWatchは、アプリケーションを監視し、システム全体のパフォーマンスの変化に対応し、リソース利用を最適化し、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。モニタリングデータと運用データをログ、メトリクス、イベントの形で収集し、AWSのリソース、アプリケーション、AWSとオンプレミスのサーバー上で動作するサービスの統一的なビューを提供します。CloudWatchは、環境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、問題のトラブルシューティングを行い、アプリケーションをスムーズに稼働させるための洞察を発見することができます。

PrometheusのメトリクスはCloudWatchで収集することもでき、アプリケーションのパフォーマンス低下や障害の監視、トラブルシューティング、アラートをより迅速に行うことができます。

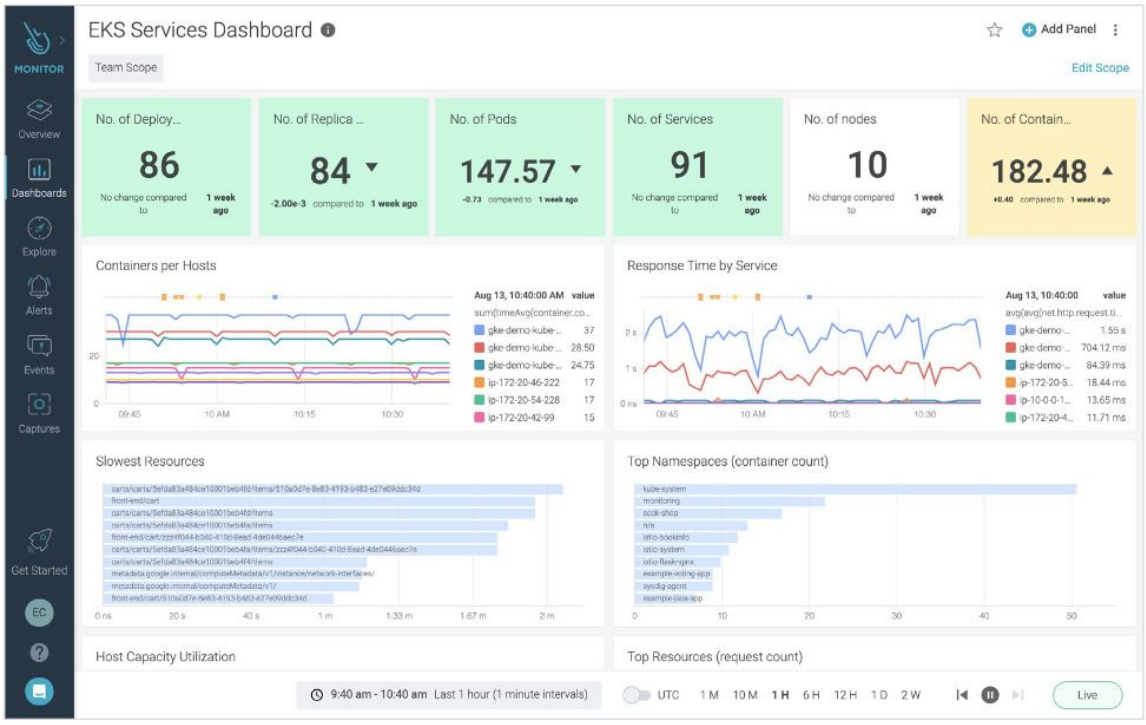
Sysdig が追加したのは....

Sysdig Monitorを使用すると、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することができます。Prometheusと完全に互換性のあるスケールでのクラウド監視を提供し、急速に変化するコンテナ環境への深い可視性を提供します。クラウドとKubernetesのコンテキストで強化された実際のシステムコールから得られる粒度の高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監視のためにチーム間でデータを統一することで、サイロを取り除くこともできます。

Kubernetesとコンテナの監視

Sysdigを使用すると、クラウドチームは、クラスタ、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とパフォーマンス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へ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、アプリケーションへの深い可視性により、健全性とパフォーマンスを監視します。Kubernetesオーケストレーションのモニタリングでクラスタの運用状況を取得します。
- コンテナとクラウドのコンテキストを使用して、問題解決のための所有者を即座に特定します。
- 過剰なリソースを消費しているポッドを特定し、キャパシティ制限を監視します。
- 自動スケーリングの動作を監視することで、予期せぬ課金やアプリケーションのロールアウト、デプロイのロールバックを制御します。
- クラスタとクラウド全体のキャパシティを最適化することで、コストを削減します。



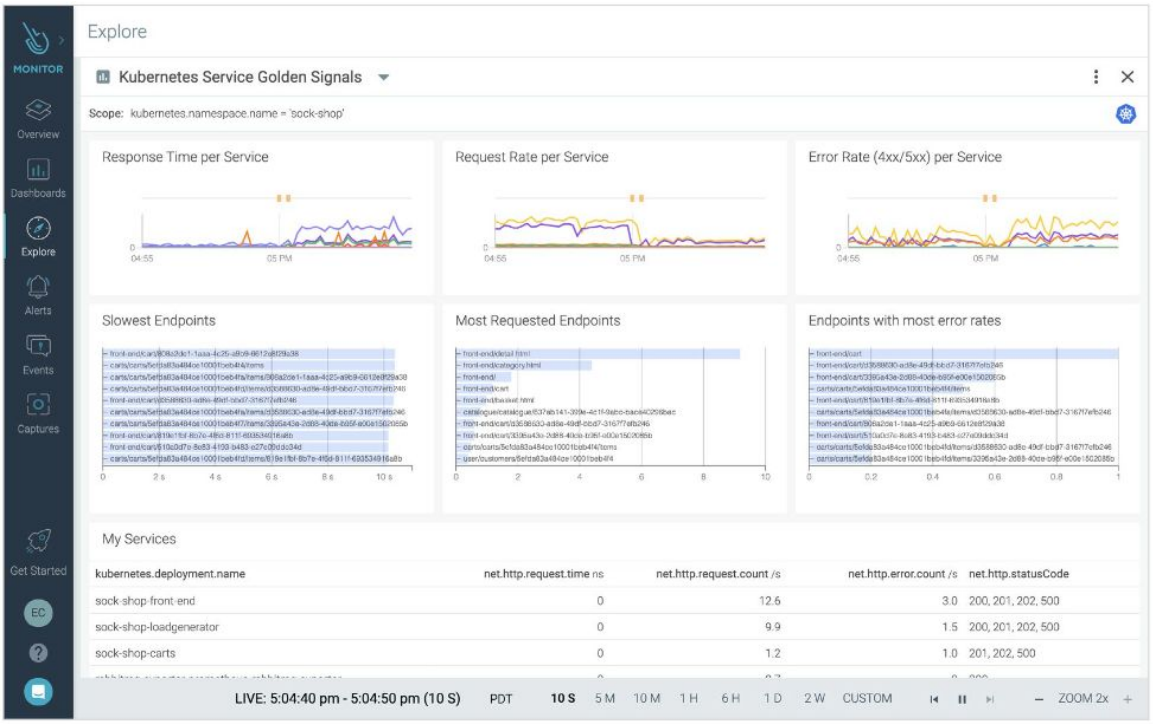
アプリケーションとサービスの監視

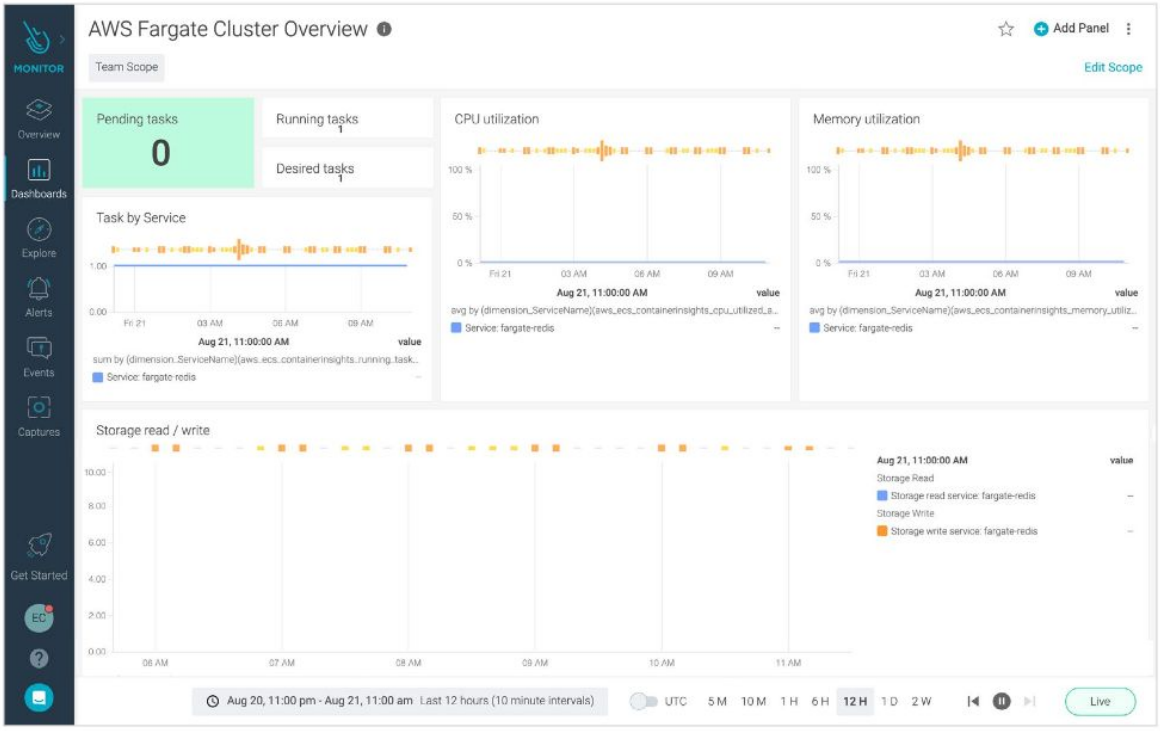
遅延、エラー、トラフィック、および左サチュレーションのメトリクスは、サービスの健全性を監視するためのゴールデン・シグナルとして知られています。これらのメトリクスは、サービスを利用するユーザーが見たアプリケーションの実際の健全性とパフォーマンスを示します。本当に重要なものを見て、アプリケーションの本当の問題を覆い隠してしまうようなトラップを回避することで、時間を節約できます。

Sysdig Monitorは以下のことを可能にします：

- 深いコンテナの可視性とKubernetesとクラウドのコンテキストで強化された粒度の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、問題を迅速に解決します。
- 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の可用性に与える影響を監視します。

- チーム、SSO、RBACなど、監視システムにエンタープライズグレードのアクセスコントロールを利用してリスクを低減します。
- 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。DevOpsチームは、スケーリングの課題に直面することなく、開発者が好む業界標準を使用することができます。
- PromCat.ioは、Kubernetesプラットフォームとクラウドネイティブサービスのための、キュレーションされ、ドキュメント化され、サポートされているモニタリング統合を含むPrometheus統合のリソースカタログです。
- Prometheus互換のエクスポート、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監視を拡張します。すぐに使えるダッシュボード（PromQLおよびGrafanaダッシュボードを含む）は、クラウドサービス、データベース、およびアプリケーション環境のその他の主要コンポーネントからのメトリクスを表示します。
- アプリケーションの可用性とセキュリティに関する単一の真実のソースにより、洞察に至る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ができます。





Sysdigでは、Amazon CloudWatchでPrometheusをより使いやすくするために、多くのAWSサービスをサポートしています。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) in Promcat.ioのサポート、エンタープライズクラスのPrometheus監視のためのオープンソースリソースカタログなどが挙げられます。

PromCat.ioには、異なるAWSサービスのAWS CloudWatchメトリクスを抽出するためのPrometheusエクスポーター機能を活用した、AWSサービスのためのキュレーションされた設定、ダッシュボード、アラート、レコーディングルールのコレクションがあります。Sysdig Monitor は、CloudWatch エクスポーターから提供されるものを含む、本番レベルの Prometheus メトリクスを統合し、スケールアップすることができます。これらのメトリクスは、あらかじめ構築されたSysdigやGrafanaのダッシュボードを使用して可視化することができます。メリットは以下の通りです。

- Prometheusへの投資を維持する：Prometheusに投資した開発者がCloudwatchも必要としている場合、Sysdigを利用することでPrometheusとPromQL言語への投資を維持することができます。

- コンテナの採用を加速します：ドキュメントで検証されたサポートを持つことで、Prometheusの統合の調査やメンテナンスに費やす開発者の時間を減らすことができ、数週間の労力を節約できます。
- より深いクラウドネイティブの可視性：より多くのメトリクスを求める開発者は、Amazon CloudWatchと連携してPrometheusを使用することで、AWSマネージドサービスを含む環境全体の可視性を得ることができます。

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のようなサービスメッシュソリューションは、コンテナ上に構築されたマイクロサービスインフラストラクチャーの次の中核的な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、認証、ロードバランシング、暗号化、トレーシングなどの機能により、コンテナ化されたマイクロサービスをより効率的にスケールで実行、管理、監視するのに役立ちます。

AWSが提供する...

AWS App Meshは、ECS、EKS、Fargate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上で稼働しているマイクロサービスの監視と制御を簡単に行うことができます。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提供し、アプリケーションの高可用性の確保を支援します。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を単一のビューで表示し、単一の制御ポイントを提供します。

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

Sysdigが追加したのは...

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稼働しているマイクロサービスがどのようにパフォーマンスを発揮しているのか、セキュリティプロファイルやサービスメッシュの全体的な健全性についてのさらなる可視性を提供します。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、インフラ全体のパ

フォーマンスとセキュリティのメトリクスを見ることができ、コンテナ化された環境をさらにコントロールすることができます。

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プする機能により、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、アラートを出し、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、充実させている膨大な量のメトリクスと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 1 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。

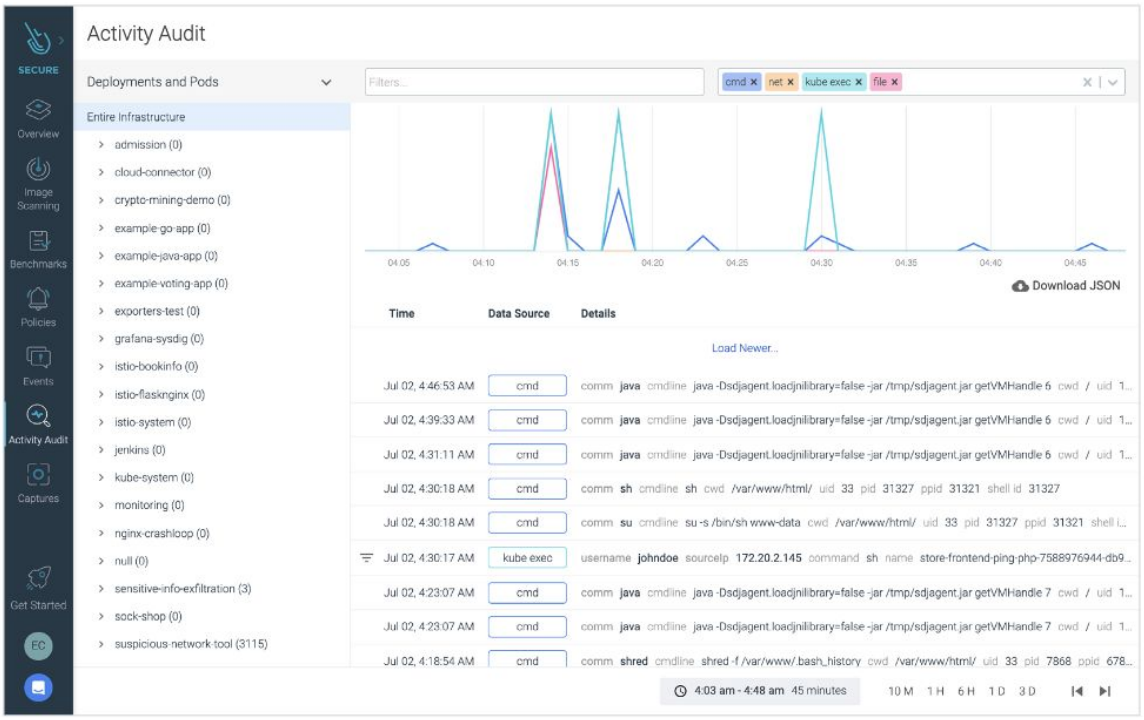
EKSやECSのようなコンテナソリューションでは、このようなことが常に起こります。コンテナはノード間で移動することができ、サービスはスケーリングされ、コンテナ・インスタンスは削除されます。問題の根本原因を特定し、問題が悪意のある活動から来ているのか、アプリの設定ミスから来ているのかを認識する能力が必要です。

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、動的な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。コンテナは儚い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のかを分析することは困難です。侵入者が取った手順をどうやって再現するのか？どのようにしてアクセスしたのか？どのような影響がありましたか？マルウェアをインストールしたか？データは流出しましたか？攻撃はどこまで拡大しましたか？

Sysdigが追加したのは...

Sysdigのアクティビティ監査は、インシデント対応を迅速化し、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て関連付けることで、SOCチームは何が起こったかを特定することができます。また、Sysdigのキャプチャーでは、スポーンされたプロセス、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ができるので、イベントを詳細に把握し、コンテナがなくなってからもKubernetesのフォレンジックを実施することができます。

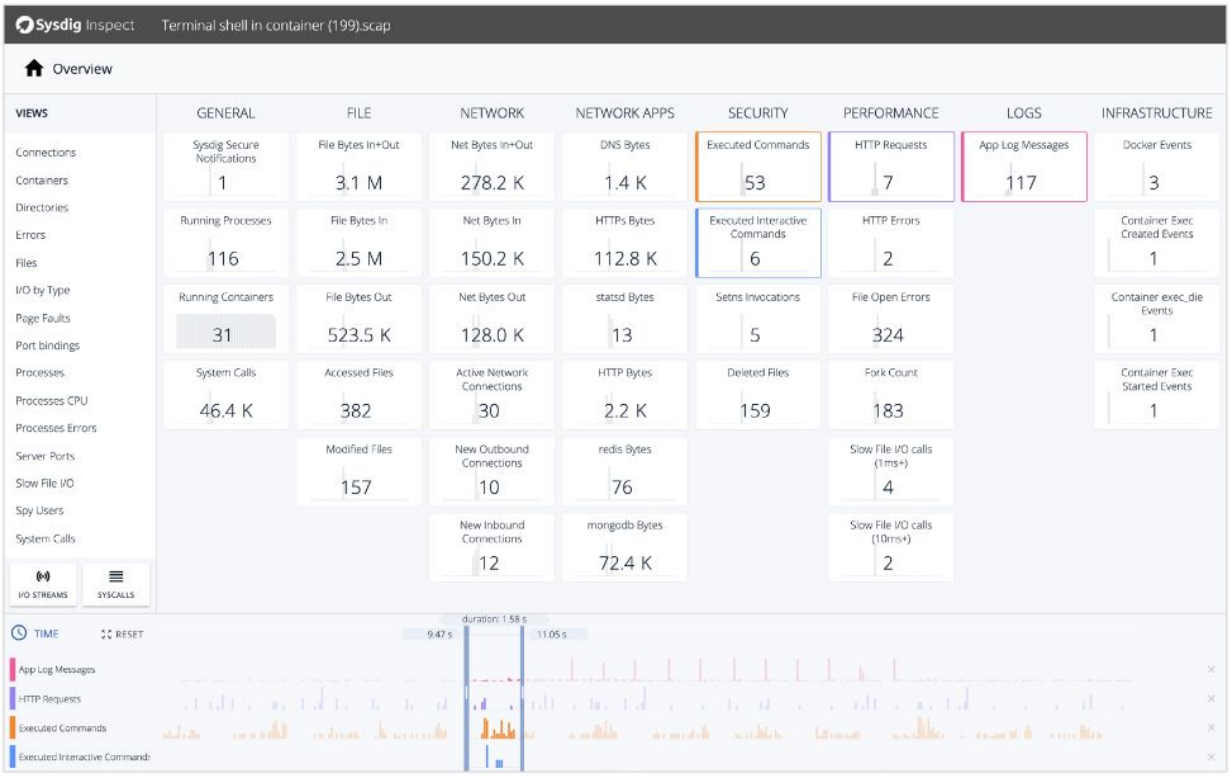


Sysdigのアクティビティ監査でKubernetesでのインシデント対応の続きを読む

Sysdigはアラートチャネル、AWS SNS、SIEMに通知を配信します。これにより、コンテナ環境全体でセキュリティの知見を集約することができるので、セキュリティアラートの表示と管理、AWSアカウント全体で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はどちらもFireLensを介してCloudwatchにイベントを送信しますが、これはFalcoによるマルチクラスターセキュリティとEKS & ECSによるAWS Firelensで見られるように、Sysdig SecureではFireLensを介してCloudwatchにイベントを送信します。

Sysdigを利用することで、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と相関のあ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することができます。Sysdigは提供しています：

- 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理解し、その影響を封じ込めることができます。
- インシデント対応を合理化し、詳細なアクティビティの記録で何が起こったのかを迅速に判断します。詳細なポリシーは、Falcoルールライブラリを活用して、ランタイムポリシー違反の分析と監査を行います。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、またはイベントを含む侵入時のステップを簡単に再現できるので、データの流出、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。
- 本番環境の外でコンテナの事後分析。これにより、AWSコンテナサービスのコンテナポッドがとっくになくなっている場合でも、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作成することができます。



AWSコンテナサービス＋Sysdig Secure DevOps Platformとの連携でより良いものに

SysdigとAWSは、顧客がECSとEKSの上に構築されたアプリケーションに簡単に移行できるようにするために設計された長いパートナーシップを結んでいます。Sysdig Secure DevOps Platformは、AWSの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やクラウドチームが、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。

これらの統合はすべて、Sysdigがコンテナコンピテンシーを持つ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サポートしており、お客様がAWS上でより良いコンテナワークロードを実行できるように支援しています。

AWSコンテナサービス上にクラウドアプリケーションを構築する際に、開発者、プラットフォーム運用、セキュリティチームが留意しなければならないセキュリティと監視のレイヤーは、いくつかの異なるものがあります。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です。

コンテナプラットフォーム

プラットフォーム	AWS	Sysdig+AWSのベネフィット
Kubernetes	Amazon Elastic Kubernetes Service (EKS)	コンテナアプリケーションの運用・監視・セキュリティ・コンプライアンスを自動化し、クラウドアプリケーションの出荷を高速化
クラウドコンテナ	AWS Elastic Container Service (ECS)	コンテナアプリケーションの運用、監視、セキュリティ、コンプライアンスを自動化し、

		クラウドアプリケーションの出荷を高速化します

セキュリティ

セキュリティレイヤー	AWS	Sysdig+AWSのベネフィット
ホストOS	Amazon Linux 2, Bottlerocket	基盤となるEC2ホスト構成を継続的にスキャンし、それがCISベンチマークに適合していることを確認します。
アクセスコントロール	AWS Identity and Access Management (IAM)	サービスベースのアクセス制御を導入し、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	Amazon ECR scanning with Clair (Package Image scanning)	CI/CDパイプラインやサポートされているレジストリ（ECR、CloudBuild、CloudPipeline、Quay、DockerHubなど）内で事前にイメージをスキャンします。Sysdigはまた、新しいCVEの影響を評価するためのランタイム脆弱性レポートも提供します。
コンプライアンス	AWS Config - evaluates the configuration settings of your AWS resources	PCI、GDPR、NIST、HIPAAなどの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。
ファイル整合性監視		Sysdig Secure ファイルシステムポリシーを使用すると、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簡単にできます。
ランタイム検出と脅威の防止		任意のAWS、ECS、およびEKSのラベル/メタデータに基づいてランタイムポリシーをスコープし、異常な動作を検出して防止します。 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た攻撃の検出とブロック 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。
コンテナフォレンジック		ECSやECSがコンテナ/ポッドを終了した後も、フォレンジックと事後分析を実施する。

監視／可視化

監視	AWS	Sysdig+AWSのベネフィット
イベントフォワード	AWS FireLens	コンテナやKubernetesのセキュリティイベント通知をAWS CloudWatchにストリーム配信し、コンプライアンスや監査のための情報を一元化します。
サービスメッシュ可視化	AWS App Mesh	App Mesh デプロイメントのパフォーマンス、健全性、セキュリティプロファイルについての洞察を得ることができます。
クラウドサービスメトリクス	Amazon CloudWatch	監視を統合して、RDS、Fargate、S3などのサービスのCloudWatchメトリクスを可視化し、複数のメトリクスソースと相関させることで、問題を迅速に特定して解決することができます。

まとめ

AWSのコンテナサービスは、コンテナプラットフォーム全体のセキュリティと監視のベースライン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ーの数をスケールアウトしていくと、Sysdigは一元化された可視性とセキュリティを提供し、既存のAWSのサービスを補完します。

Sysdigは、AWSのお客様をサポートするための実績ある経験、信頼性、技術的な熟練度を持っています。Sysdig Secure DevOps Platformは、AWSのコンテナサービス上にセキュリティを埋め込み、可用性を最大化し、コンテナライフサイクル全体でコンプライアンスを検証するために企業が求めるスケール、パフォーマンス、ユーザビリティを提供します。

追加リソース

パートナーシップ概要

- Sysdig/AWSパートナーシップ概要

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
- LogDNA：SysdigによるAWS EKS上のコンテナの監視とセキュリティの確保
- Sunrun: AWS ECSのためのコンテナインテリジェンス

Webinar:

- AWS Security 101: Securing Amazon EKS with Falco & Sysdig
- AWS Observability 101: Kubernetes and Prometheus Monitoring with Sysdig
- Best Practices to Secure Containers and Accelerate Software Delivery

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

© 2020 Sysdig, Inc. 無断複写・転載を禁じます。ガイド010 Rev.B 9/20(日本語)