コンテナおよびKubernetesにおけるPCIコンプライアンスガイド

ドキュメントバージョン 1.2

本文の内容は、「A guide to PCI Compliance in Containers and Kubernetes」
https://sysdig.com/resources/whitepapers/a-guide-to-pci-compliance-in-containers-and-kubernetes/
を元に日本語に翻訳・再構成した内容となっております。

はじめに

以前は、クレジットカード会社は、カード会員データを保存、処理、または送信するすべてのベンダーに対して、独自のバージョンのコンプライアンスを実施する必要がありました。その後、2000年代初頭に、アメリカンエクスプレス、JCB、ビザ、ディスカバー、マスターカードの代表者が集まり、ペイメントカード業界セキュリティ基準審議会（PCI SSC）を設立しました。 この評議会はPCI DSS（ペイメントカード業界データセキュリティサービス）を作成し、2006年に最初の標準セットをリリースしました。

標準の最新バージョンであるPCI DSS 3.2.1は2018年5月に発表されました。標準はガイドラインとして機能し、組織がコンプライアンス戦略を構築するための出発点となりました。 アプリケーションとテクノロジーの変化に伴い、組織はPCI DSSによって設定されたガイドラインを満たすためにコンプライアンス戦略を適合させる必要があります。

PCI DSSはどこに適用するのか？

「PCI DSSセキュリティ要件は、カード会員データ環境に含まれる、またはそれに接続されるすべてのシステムコンポーネントに適用されます。」

カード会員データ環境（CDE）は、カード会員データまたは機密認証データを保存、処理、または送信する人、プロセス、および技術で構成されています。 「システムコンポーネント」には、ネットワークデバイス、サーバー、コンピューティングデバイス、およびアプリケーションが含まれます。 これらのアプリケーションの多くは、現在コンテナで直に稼働しています。

コンテナ、KubernetesおよびPCIコンプライアンス

コンテナは、これまでのエンタープライズテクノロジーよりも急速に採用されており、それには正当な理由があります。 移植性があり、分離によりセキュリティが向上し、アプリケーションチームはより優れたサービスをより迅速に開発できます。しかしながら、急速に採用が進んでいるペースに対してコンプライアンスサイドからは適合させるのは非常に困難です。 代表的な例としては、用語集、略語、およびV3.2 PCI-DSSガイドラインの頭字語です。 仮想マシン、ハイパーバイザー、およびVMの世界で知っておく必要のあるすべての定義があります。 ただし、Docker、コンテナ、オーケストレーション、Kubernetes、またはコンテナをデプロイする際にさらに重要になる（カーネル）に関する言及はありません。

コンテナを使用すると、環境全体でより高度なセグメンテーションと分離が可能になりますが、その密度とエフェメラルな性質により、ネットワーク接続の数が大幅に増加し、さらに何がどこに接続されているかを追跡がしにくくなります。この密度の増加により、脆弱性の監査とチェックが必要なエンティティの数も増加します。

PCI DSS要件

PCI DSS 3.2.1は、 12の要件カテゴリと5つの付録を定義しています。

- **要件1：カード会員データを保護するために、ファイアウォール構成を導入して維持する**
  ファイアウォールは、エンティティのネットワーク（内部）と信頼されていないネットワーク（外部）の間で許可されるコンピュータートラフィック、およびエンティティの内部の信頼されたネットワーク内の機密性の高いエリアを出入りするトラフィックを制御するデバイスです。 カード会員データ環境は、エンティティの信頼できるネットワーク内のより機密性の高い領域の一例です。
- **要件2：ベンダーが提供するシステムパスワードやその他のセキュリティパラメータのデフォルトを使用しない**
  悪意のある個人（エンティティの外部および内部）は、多くの場合、ベンダーのデフォルトパスワードおよびその他のベンダーのデフォルト設定を使用して、システムを侵害します。これらのパスワードと設定はハッカーコミュニティでよく知られており、公開情報を介して簡単に入手されます。
- **要件3：保存されたカード会員データを保護する**
  暗号化、切り捨て、マスキング、ハッシュなどの保護方法は、カード会員データ保護の重要なコンポーネントです。侵入者が他のセキュリティコントロールを回避しても、適切な暗号化キーなしで暗号化されたデータにアクセスした場合、そのデータは読めず、使用できません。 格納されたデータを保護する他の効果的な方法も、潜在的なリスク軽減の機会と見なされる必要があります。たとえば、リスクを最小限に抑える方法には、どうしても必要な場合を除いてカード会員データを保存しない、完全なPANが不要な場合はカード会員データを切り捨てる、電子メールやインスタントメッセージングなどのエンドユーザーメッセージングテクノロジーを使用して保護されていないPANを送信しないことが含まれます。
- **要件4：オープンなパブリックネットワークを介したカード会員データの送信を暗号化する**
  機密情報は、悪意のある個人が簡単にアクセスできるネットワークを介したやりとりにおいて暗号化する必要があります。誤った設定のワイヤレスネットワーク、レガシー暗号化およ

び認証プロトコルの脆弱性は、脆弱性を悪用してカード会員データ環境への特権アクセスを取得する悪意のある個人の標的となります。

- **要件5：すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する** ー
  般的に「マルウェア」と呼ばれる悪意のあるソフトウェア（ウイルス、ワーム、トロイの木馬など）は、従業員の電子メールやインターネット、モバイルコンピューター、ストレージデバイスなど、ビジネスで承認された多くの活動中にネットワークに入り込み、システムの脆弱性を悪用します。 現在および進化する悪意のあるソフトウェアの脅威からシステムを保護するために、マルウェアの一般的な影響を受けるすべてのシステムでウイルス対策ソフトウェアを使用する必要があります。追加のマルウェア対策ソリューションは、ウイルス対策ソフトウェアの補足と見なすことができます。ただし、このような追加のソリューションは、ウイルス対策ソフトウェア配備の必要性を置き換えるものではありません。
- **要件6：安全なシステムとアプリケーションの開発および維持** 悪
  意のある個人は、セキュリティの脆弱性を使用してシステムへの特権アクセスを取得します。 これらの脆弱性の多くは、ベンダーが提供するセキュリティパッチによって修正されます。セキュリティパッチは、システムを管理するエンティティがインストールする必要があります。すべてのシステムには、悪意のある個人および悪意のあるソフトウェアによるカード会員データの悪用および侵害から保護するために、適切なソフトウェアパッチがすべて必要です。
- **要件7：ビジネスによって必要とする場合のみに、カード会員データへのアクセスを制限する**
  重要なデータに権限のある人のみがアクセスできるようにするには、システムとプロセスを配備して、知る必要性と職責に基づいてアクセスを制限する必要があります。
- **要件8：システムコンポーネントへのアクセスを識別し、認証する**
  アクセス権を持つ各個人に一意の識別（ID）を割り当てることにより、すべての個人が自分のアクションに対して一意に責任を負うことが保証されます。このような説明責任がある場合、重要なデータとシステムに対して実行されるアクションは、既知の承認されたユーザーとプロセスによって実行され、追跡できます。
- **要件9：カード会員データへの物理的アクセスを制限する**
  カード会員データを格納するデータまたはシステムへの物理的なアクセスは、個人がデバイスまたはデータにアクセスし、システムの削除またはハードコピーを行う機会を与えるため、適切に制限する必要があります。要件9の目的で、「オンサイト要員」とは、エンティティの敷地内に物理的に存在するフルタイムおよびパートタイムの従業員、臨時従業員、請負業者およびコンサルタントを指します。「訪問者」とは、ベンダー、オンサイト要員のゲ

スト、サービス労働者、または施設に短時間（通常は1日以内）入場する必要がある人を指します。「メディア」とは、カード会員データを含むすべての紙および電子メディアを指します。

- **要件10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する**
  ロギングメカニズムとユーザーアクティビティを追跡する機能は、データ侵害の影響を防止、検出、または最小化するために重要です。すべての環境にログが存在するため、何か問題が発生した場合に徹底的な追跡、アラート、分析が可能です。システムアクティビティログがないと、侵害の原因を特定することは不可能ではないにしても、非常に困難です。
- **要件11：セキュリティシステムとプロセスに対して定期的にテストを行う**
  脆弱性は悪意のある個人や研究者によって継続的に発見されており、新しいソフトウェアによって発見されています。システムコンポーネント、プロセス、およびカスタムソフトウェアは、セキュリティ管理が変化する環境を反映し続けることを確認するために頻繁にテストする必要があります。
- **要件12：すべての担当者の情報セキュリティに対処するポリシーを維持する**
  強力なセキュリティポリシーは、エンティティ全体のセキュリティトーンを設定し、それらに期待されることを担当者に通知します。すべての担当者は、データの機密性とそれを保護する責任を認識している必要があります。要件12の目的で、「職員」とは、エンティティのサイトに「常駐」しているか、カード会員データ環境にアクセスできる、フルタイムおよびパートタイムの従業員、臨時従業員、請負業者、およびコンサルタントを指します。
- **付録A1**：共有ホスティングプロバイダーにおける追加のPCI DSS要件
- **付録A2**：カードプレゼンスPOS POI端末接続においてSSL/初期のTLSを使用するエンティティにおける追加のPCI DSS要件
- **付録A3**：指定されたエンティティの補足検証（DESV）
  この付録は、既存のPCI DSS要件の追加検証を必要とするペイメントブランドまたは加盟店契約会社によって指定された事業体にのみ適用されます。
- **付録B**：代替コントロール
  正当な技術的または文書化されたビジネス上の制約により、エンティティが明示的に要件を満たせない場合、ほとんどのPCI DSS要件について、代替コントロールを検討できますが、他のコントロールまたは代替コントロールを実装することにより、要件に関連するリスクを十分に軽減します。
- **付録C**：代替コントロールワークシート

機能カバレッジ

このガイドでは、以下に関連するPCIコンプライアンスについて説明します。

- ネットワークセキュリティー
- データ保護
- 監査
- ユーザーアクセス制御
- インシデント対応と復旧
- フォレンジック
- 脆弱性管理

特定の要件ごとに、ガイドライン、コンテナ環境の要件に対処する方法、およびSysdigがどのように役立つかについて説明します。

要件とSysdigの機能

要件1：

カード会員データを保護するためのファイアウォール構成を導入して維持する

ファイアウォールは、エンティティのネットワーク（内部）と信頼されていないネットワーク（外部）の間で許可されるコンピュータートラフィック、およびエンティティの内部の信頼されたネットワーク内の機密性の高いエリアを出入りするトラフィックを制御するデバイスです。 カード会員データ環境は、エンティティの信頼できるネットワーク内のより機密性の高い領域の一例です。

1.1.2 現在のネットワーク図

要件

カード会員データ環境とワイヤレスネットワークを含む他のネットワークとの間のすべての接続を識別する現在のネットワーク図

ガイドライン

ネットワーク図は、ネットワークの構成方法を説明し、すべてのネットワークデバイスの場所を識別します。現在のネットワーク図がなければ、デバイスは見過ごされ、知らないうちにPCI DSSに実装されたセキュリティコントロールから除外される可能性があり、したがって侵害に対して脆弱となり得ます。

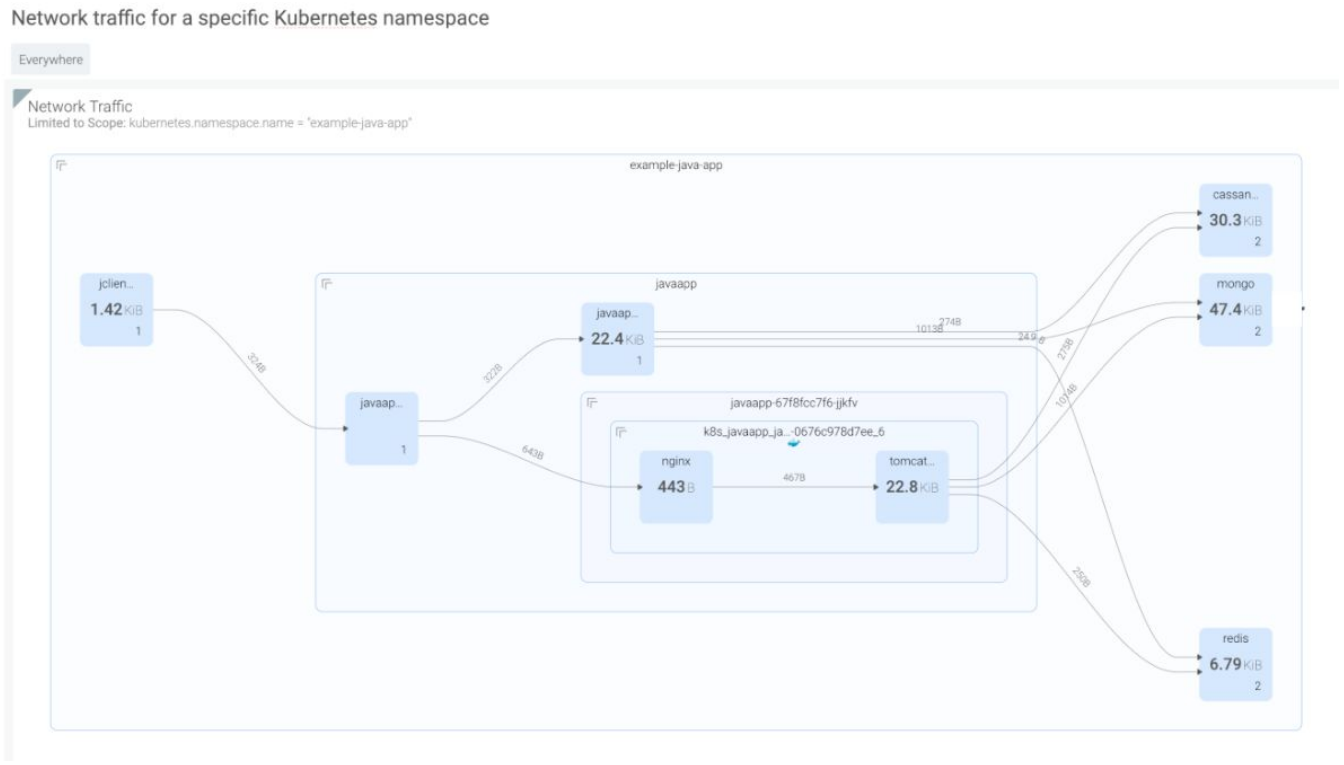
コンテナコンプライアンスアプローチ

APIサービスは、単なる数個のノードのコレクションではなく、数十または数百のノードと、他のサービスが実行されている数千のコンテナに分散しています。これらの分散コンテナ化サービスでは、誰が誰と話しているのか、そしてその理由を追跡するのは非常にに困難です

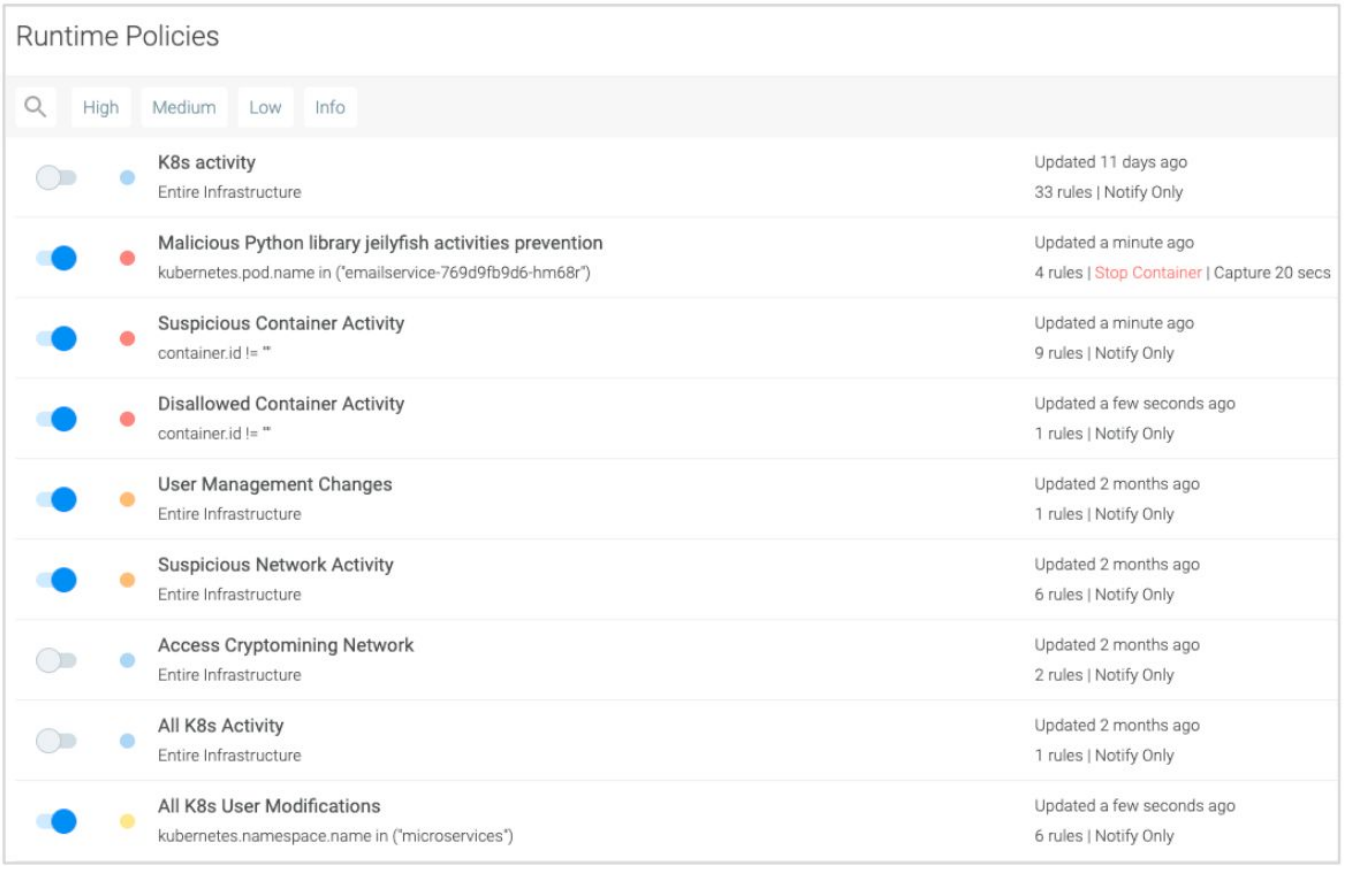
Sysdigの機能

Sysdigは、CDE環境と非CDE環境のすべてのコンテナ、ホスト、およびプロセスを示すリアルタイムトポロジマップを使用して、コンテナとKubernetesノードおよびサービスの自動検出を提供します。 Sysdigはすべての接続をリアルタイムで監視し、コンテナとの新しい接続をすぐに検出しま

す。



Sysdigでは、そのポリシーに適用される物理的または論理的なスコープに基づいて、ネットワークおよびその他のサービスを保護するポリシーを表示することもできます。これにより、PCIコンプライアンス戦略のさまざまな領域にどのポリシーが適用されるかを追跡しやすくなります。



ランタイムポリシーリストには、有効なポリシーを示すスイッチが表示され、その名前の下に、適用される場所を指定するスコープ定義が表示されます。

1.1.3 データフロー図

要件

システムおよびネットワーク全体のすべてのカード会員データフローを示す現在の図

ガイドライン

チームは、データフロー図を調べて、システムおよびネットワーク全体のすべてのカード会員データフローを視覚化する必要があります。

Sysdigの機能

Sysdigは、コンテナとサービス間のリアルタイムネットワーク接続を自動的に検出します。 チームは、コンテナおよびKubernetesメタデータ/ラベルに基づいて、特定の異常なフローをCDEおよび非CDEとしてアラートすることもできます。

1.1.5 グループ、役割、責任の記述

マネジメントネットワークコンポーネント

要件

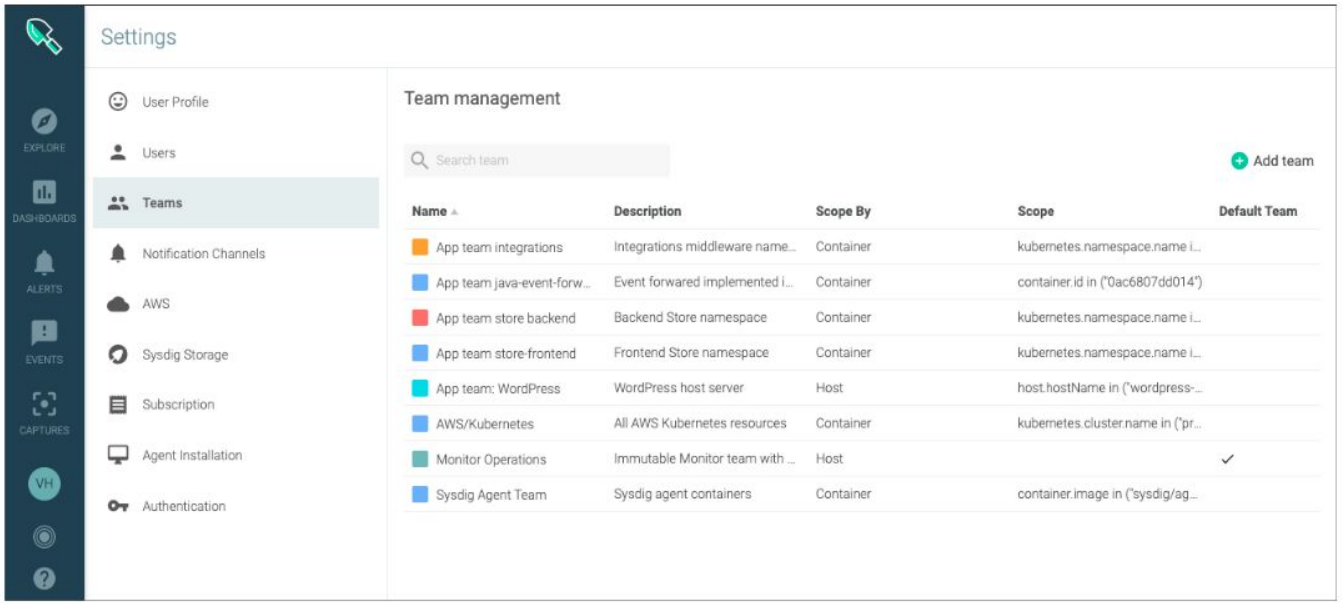
ネットワークコンポーネントの管理に関するグループ、役割、および責任の説明。

ガイドライン

チームは、ファイアウォールおよびルーターの構成標準に、ネットワークコンポーネントの管理に関するグループ、役割、および責任の説明が含まれていることを確認する必要があります。

Sysdigの機能

Sysdigは、Sysdigチームと呼ばれるサービスベースのアクセスコントロールを提供し、PCIコンテナ化環境のグループ、役割、および責任を管理します。Sysdigソフトウェア（オンプレミス版）プラットフォームにおけるLDAPサポートにより、顧客自身のディレクトリサーバーの資格情報を使用したユーザー認証も可能となります。



1.1.6.b 安全でないサービス、および、許可されているプロトコルとポートを特定する

要件

1.1.6.b 安全でないサービス、許可されているプロトコルおよびポートを特定し、各サービスのセキュリティ機能が文書化されていることを確認します。

ガイドライン

侵害はしばしば未使用または安全でないサービスとポートが原因で発生します。これらは多くの場合既知の脆弱性があり、多くの組織は使用していないサービス、プロトコル、ポートの脆弱性にパッチを当てていません（脆弱性がまだ存在する場合でも）。ビジネスに必要なサービス、プロトコル、およびポートを明確に定義および文書化することにより、組織は他のすべてのサービス、プロトコル、およびポートが無効化または削除されることを保証できます。

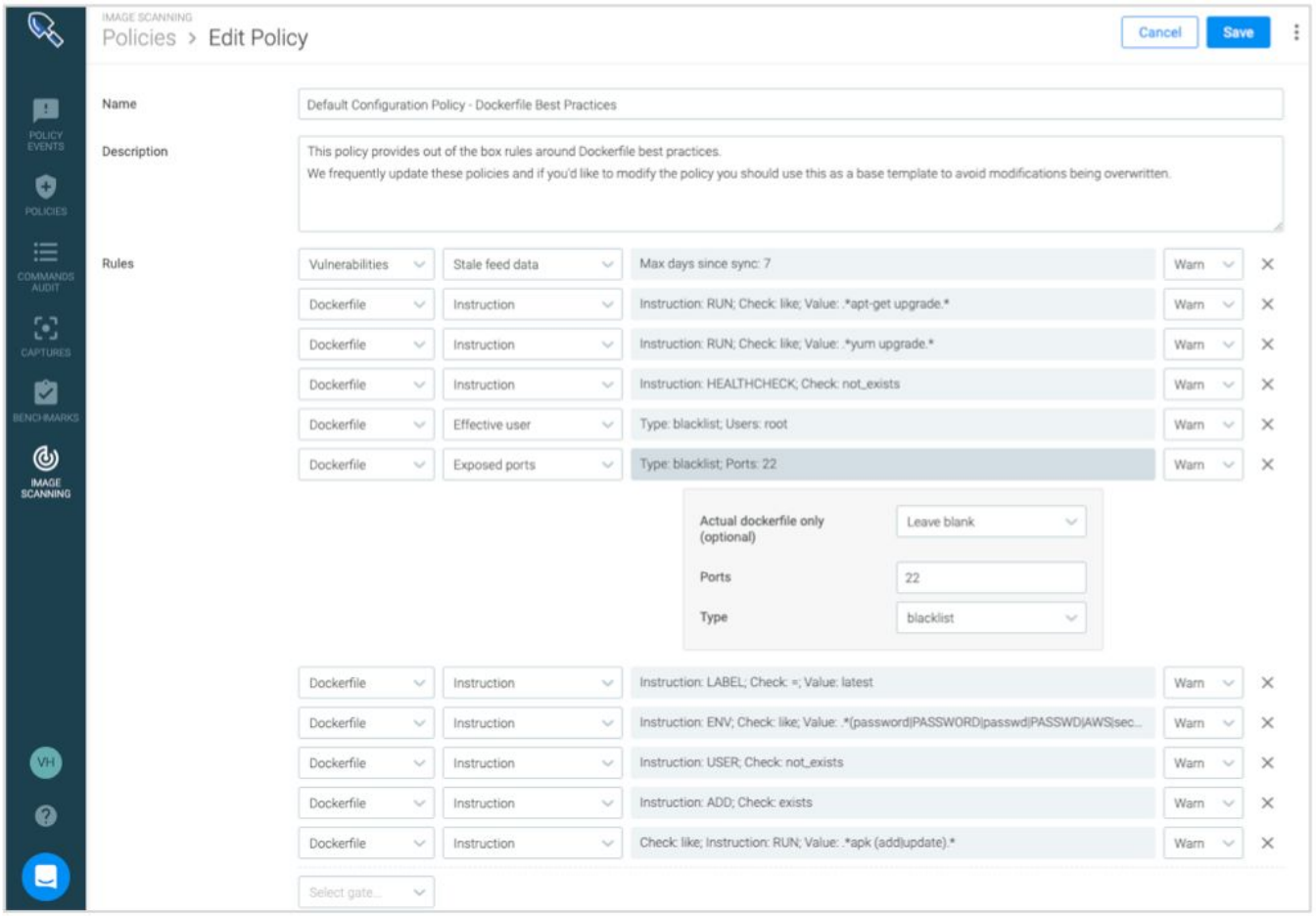
コンテナコンプライアンスアプローチ

データベースサーバーが通常使用するポートを文書化するのは簡単です。Kubernetesまたは他のオーケストレーターが同じホスト上でそれらをスケジュールしているため、そのホストにロードバランサー、アプリケーションサーバー、およびデータベースがある場合には課題が生じます。各コンテナには、ニーズに合わせて独自のポートが公開されます。チームは、不適切に公開されたポートがないことを確認する必要があります。

Sysdigの機能

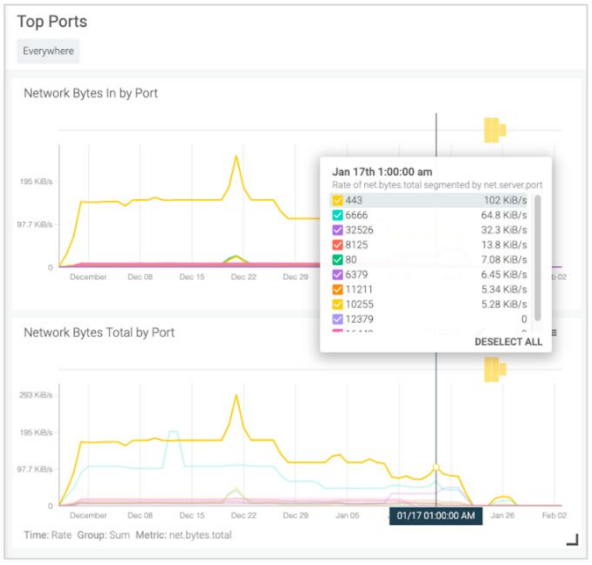
防止

Sysdigは、そのコンテナで公開されているポートに基づいて、イメージの構築またはデプロイメントを防ぐことができます。イメージのポートをホワイトリストまたはブラックリストとして簡単に選択し、それらがCI/CD評価のステップとして公開されているかどうかを評価します。



モニタリング（監視）

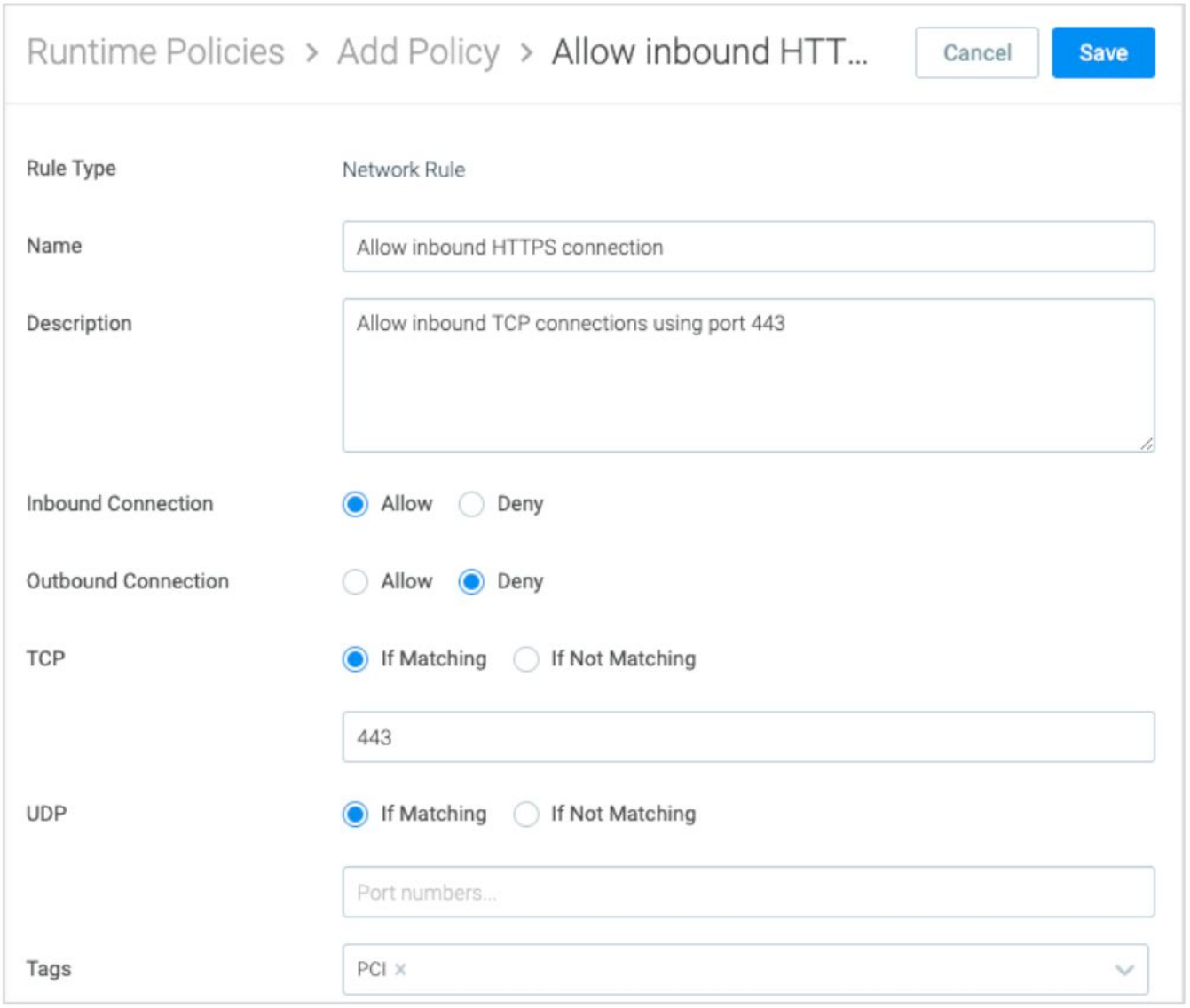
Sysdigは、ホスト、コンテナ、デプロイメント、または任意の論理サービスが使用しているポートを表示し、リクエストバイトなどに関するメトリクスを提供できます。



検出

コンテナまたはサービスの標準ポート動作を可視化した後、予期しないインバウンド/アウトバウン

ド動作を検出するポリシーを簡単に作成したり、リスニングのために開くことができるTCP / UDP ポートを制御したりできます。



要件 2:

システムパスワードおよびその他のセキュリティパラメータにベンダー提供のデフォルトを使用しない

悪意のある個人（エンティティの外部および内部）は、多くの場合、ベンダーのデフォルトパスワードおよびその他のベンダーのデフォルト設定を使用して、システムを侵害します。これらのパスワードと設定はハッカーコミュニティでよく知られており、公開情報を介して簡単に入手できます。

2.2 構成標準: CIS, ISO, SANS, NIST

要件の説明

すべてのシステムコンポーネントを構成標準で開発します。これらの標準が既知のすべてのセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化標準と一致していることを確認してください。業界で受け入れられているシステム強化標準のソースには、以下が含まれますが、これらに限定されません。

- インターネットセキュリティセンター（CIS）
- 国際標準化機構（ISO）
- SysAdmin Audit Network Security（SANS）Institute
- 国立標準技術研究所（NIST）

ガイドライン

多くのオペレーティングシステム、データベース、エンタープライズアプリケーションには既知の弱点があり、セキュリティの脆弱性を修正するためにこれらのシステムを構成する既知の方法もあります。セキュリティの専門家ではない人を支援するために、多くのセキュリティ組織がこれらの弱点を修正する方法をアドバイスするシステム強化ガイドラインと推奨事項を確立しています。

2.2.a システム構成標準

要件の説明

組織のすべてのタイプのシステムコンポーネントのシステム構成標準を調べ、システム構成標準が業界で受け入れられている強化標準と一致していることを確認します。

コンテナコンプライアンスアプローチ

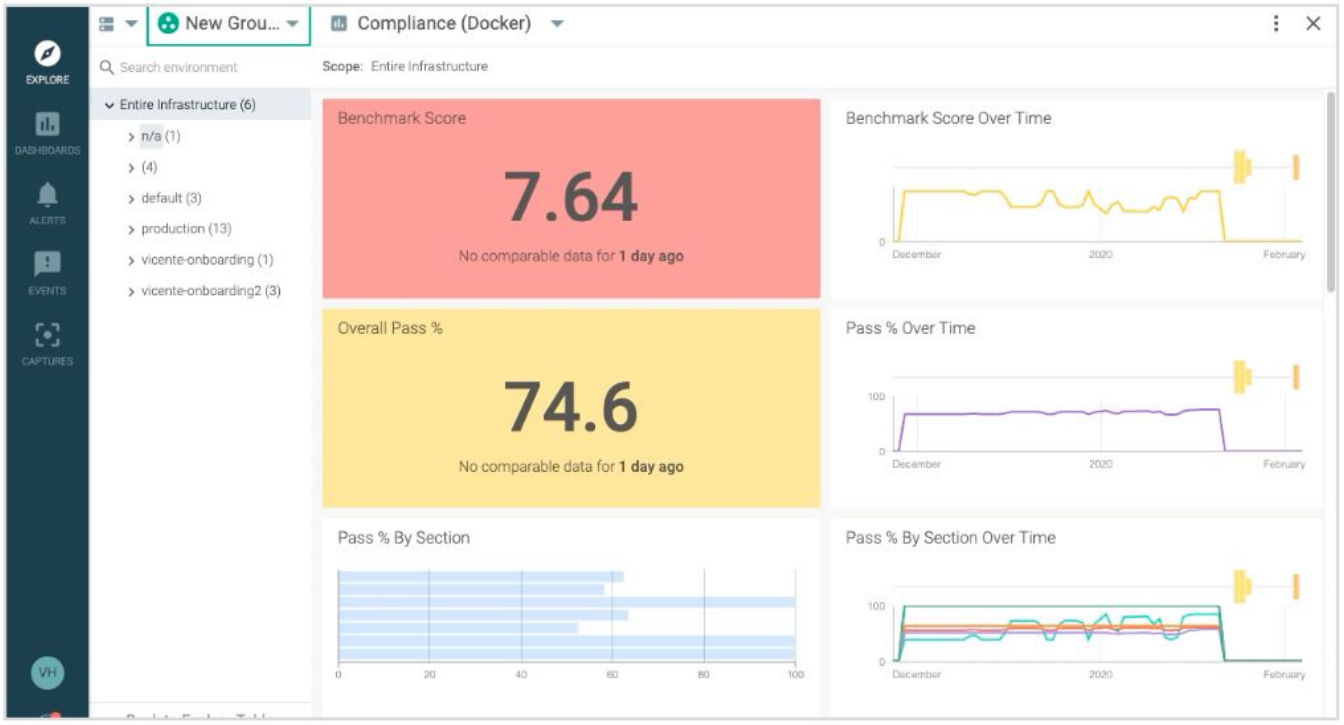
CISは、DockerおよびKubernetesを強化するためのベンチマークを公開しています。これらを使用

して、Dockerホスト、デーモン、kubernetesサービス、およびコンテナスタックの他の重要なコンポーネントの安全な構成を確認できます。

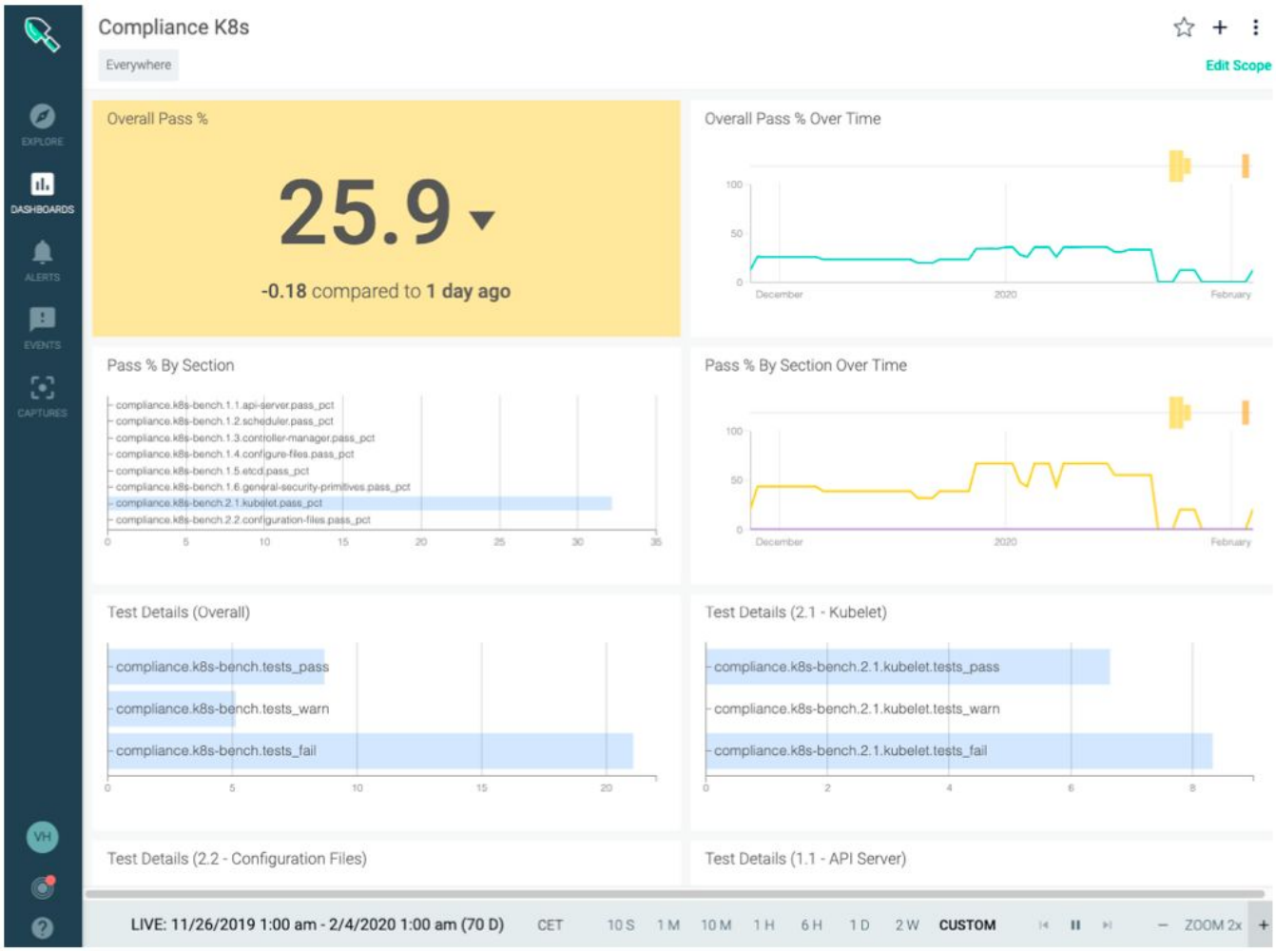
Sysdigがどのように役立つか

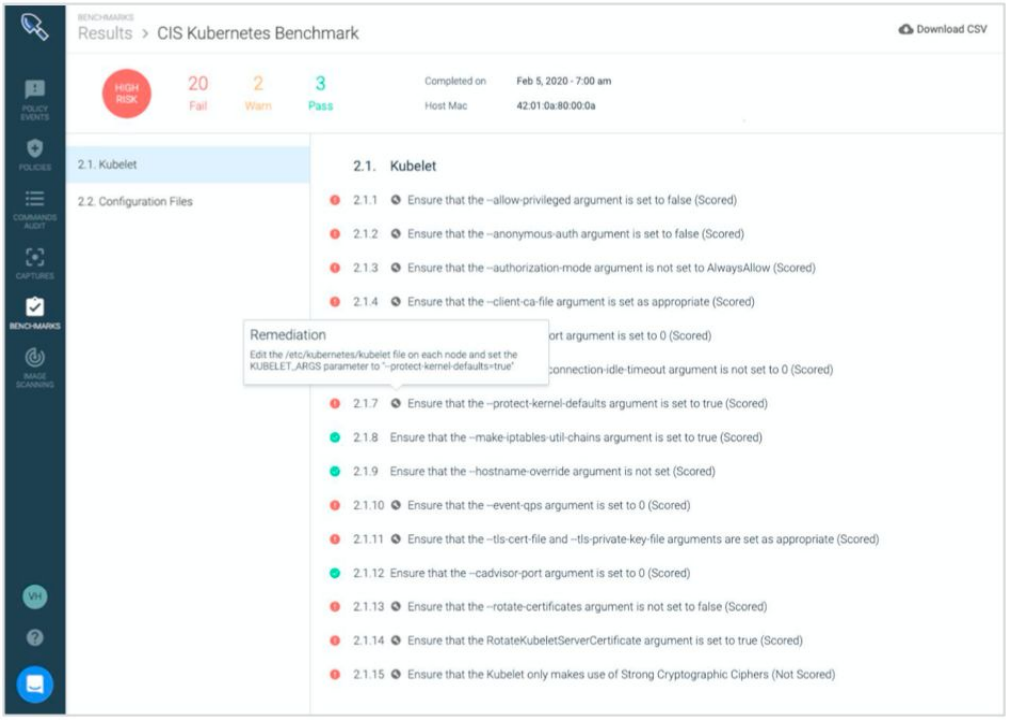
Sysdigを使用すると、ユーザーはCIS DockerベンチマークとCIS Kubernetesベンチマークをインフラストラクチャの領域で実行するようにスケジュールできます。Sysdigは、これらの結果をレポート形式で返し、ダッシュボードとアラートのメトリクスも返します。

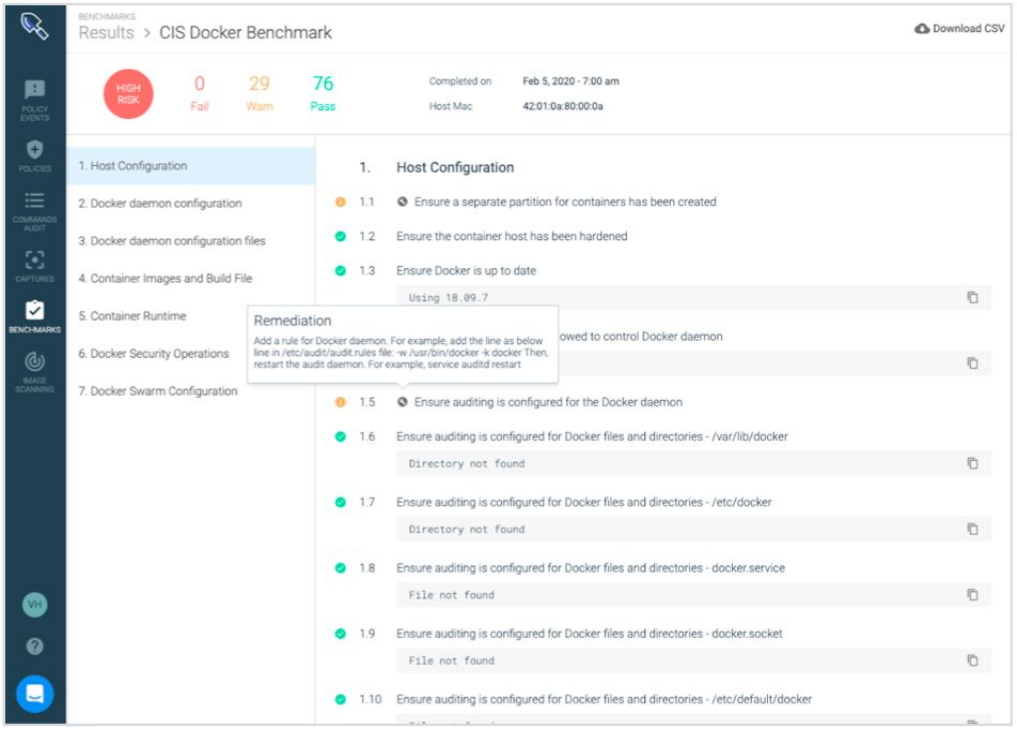
ダッシュボード



レポート


Compliance K8s
Everywhere
Edit Scope
EXPLORE
DASHBOARDS
ALERTS
EVENTS
CAPTURES
Overall Pass %
25.9
-0.18 compared to 1 day ago
Overall Pass % Over Time
100
50
0
December
2020
February
Pass % By Section
compliance.k8s-bench.1.1.api-server.pass_pct
compliance.k8s-bench.1.2.scheduler.pass_pct
compliance.k8s-bench.1.3.controller-manager.pass_pct
compliance.k8s-bench.1.4.configure-files.pass_pct
compliance.k8s-bench.1.5.etcd.pass_pct
compliance.k8s-bench.1.6.general-security-primitives.pass_pct
compliance.k8s-bench.2.1.kubelet.pass_pct
compliance.k8s-bench.2.2.configuration-files.pass_pct
0
5
10
15
20
25
30
35
Pass % By Section Over Time
100
50
0
December
2020
February
Test Details (Overall)
compliance.k8s-bench.tests_pass
compliance.k8s-bench.tests_warn
compliance.k8s-bench.tests_fail
0
5
10
15
20
Test Details (2.1 - Kubelet)
compliance.k8s-bench.2.1.kubelet.tests_pass
compliance.k8s-bench.2.1.kubelet.tests_warn
compliance.k8s-bench.2.1.kubelet.tests_fail
0
2
4
6
8
Test Details (2.2 - Configuration Files)
Test Details (1.1 - API Server)
VH
LIVE: 11/26/2019 1:00 am - 2/4/2020 1:00 am (70 D)
CET
10 S
1 M
10 M
1 H
6 H
1 D
2 W
CUSTOM
ZOOM 2x





2.2.1 サーバーごとに1つの機能に分離（コンテナ）

要件の説明

異なるセキュリティレベルを必要とする機能が同じサーバーに共存しないように、サーバーごとに

1つの主要な機能のみを実装します。たとえば、Webサーバー、データベースサーバー、DNSは別々のサーバーに実装する必要があります。

ガイドライン

異なるセキュリティレベルを必要とするサーバー機能が同じサーバーに配置されている場合、セキュリティの低い機能が存在するため、セキュリティのニーズが高い機能のセキュリティレベルが低下します。さらに、セキュリティレベルが低いサーバー機能により、同じサーバー上の他の機能にセキュリティ上の脆弱性が生じる可能性があります。システム構成標準および関連プロセスの一部として、さまざまなサーバー機能のセキュリティニーズを考慮することにより、組織は、さまざまなセキュリティレベルを必要とする機能が同じサーバーに共存しないようにすることができます。

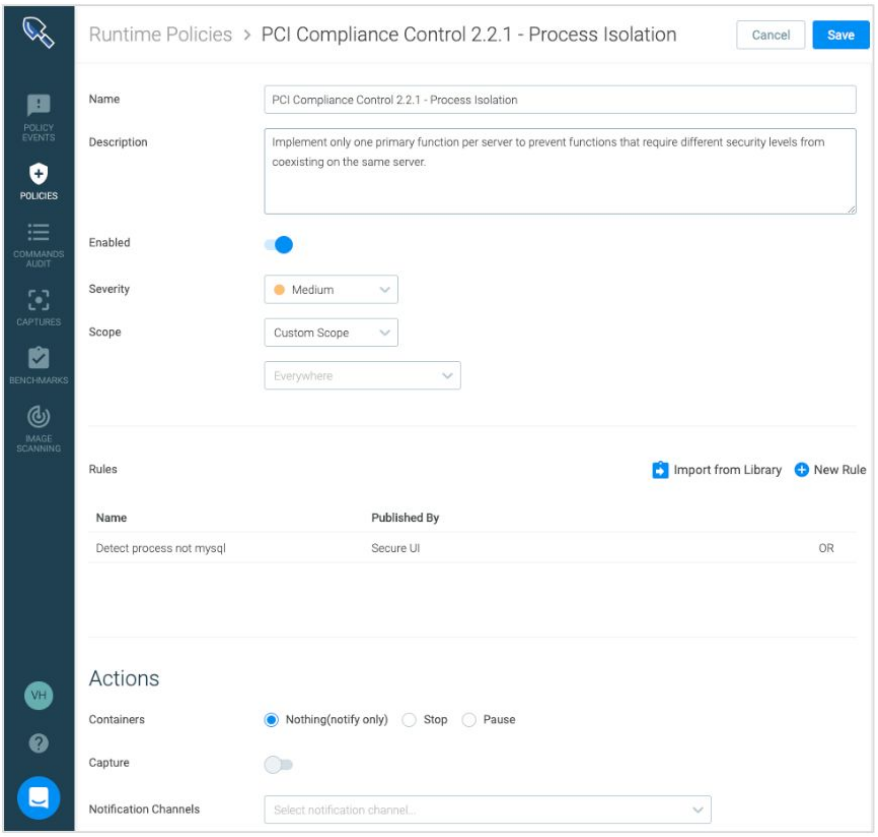
コンテナコンプライアンスアプローチ

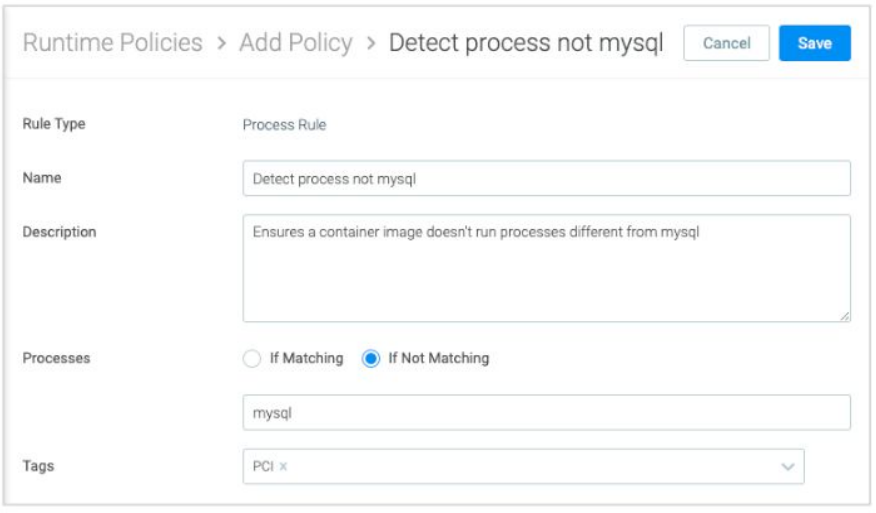
これは、コンテナが生きてくる側面です！これらを使用すると、物理インフラストラクチャをあまり気にせずに、実行中のプロセスを互いに分離できます。また、コンテナごとに1つのプロセスを実行するだけで、ワークロードを分離するためのより簡単で費用対効果の高い方法を提供します。

Sysdigがどのように役立つか

Sysdig Secureを使用すると、コンテナ内のプロセス分離に対する違反を検出するポリシーを構築し、そのポリシーに違反した場合にコンテナを強制終了できます。

プロセス分離例


Runtime Policies > PCI Compliance Control 2.2.1 - Process Isolation
Cancel
Save
POLICY EVENTS
POLICIES
COMMANDS AUDIT
CAPTURES
BENCHMARKS
IMAGE SCANNING
Name
PCI Compliance Control 2.2.1 - Process Isolation
Description
Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server.
Enabled
Severity
Medium
Scope
Custom Scope
Everywhere
Rules
Import from Library
New Rule
Name
Published By
Detect process not mysql
Secure UI
OR
Actions
Containers
Nothing(notify only)
Stop
Pause
Capture
Notification Channels
Select notification channel...


Runtime Policies > Add Policy > Detect process not mysql
Cancel
Save
Rule Type
Process Rule
Name
Detect process not mysql
Description
Ensures a container image doesn't run processes different from mysql
Processes
If Matching
If Not Matching
mysql
Tags
PCI

Falcoランタイム検出ルールは、承認されたサーバープロセスおよびポートからではないインバウンドまたはアウトバウンドトラフィックの検出も実装できます。

```
# Rule to detect inbound or outbound traffic not to authorized
# server process and port
#
# Security standards that apply to:
# PCI 2.2.1. One function per server isolation (containers)
- macro: restrict_binary_port
 condition: never_true
- macro: restrict_image
  condition: container.image.repository=nginx # change to image to monitor
- macro: authorized_server_binary
  condition: proc.name="nginx" # change to binary to allow
- macro: authorized_server_port
```

```
  condition: fd.sport="80" # change to port to allow

- rule: Outbound or inbound traffic not to authorized server process and port

  desc: Only authorized process should receive network traffic.

  condition: >

    restrict_binary_port and

    inbound_outbound and

    container and

    k8s.ns.name in (namespace_scope_remote_nodomain) and

    restrict_image and

    (not authorized_server_binary

     or not authorized_server_port)

  output: >

    Network connection outside authorized port and binary

    (command=%proc.cmdline connection=%fd.name user=%user.name
    container_id=%container.id image=%container.image.repository)

  priority: WARNING

  tags: [network, PCI, PCI_DSS_2.2.1, PCI_DSS_2.2.2]
```

2.2.2 必要なサービス、プロトコル、デーモンのみを有効にする

要件定義

システムの機能に必要な、必要なサービス、プロトコル、デーモンなどのみを有効にします。

ガイドライン

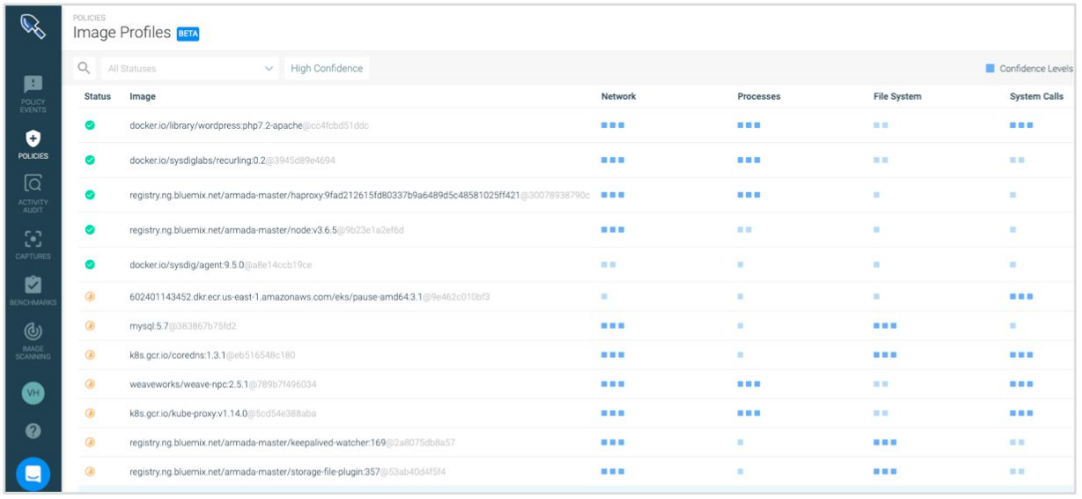
要件1.1.6で述べたように、ネットワークを危険にさらすために悪意のある個人が一般的に使用する多くのプロトコルがビジネスで必要になる（またはデフォルトで有効になっている）ことがあります。この要件を組織の構成標準および関連プロセスの一部として含めることにより、必要なサービスとプロトコルのみを有効にします。

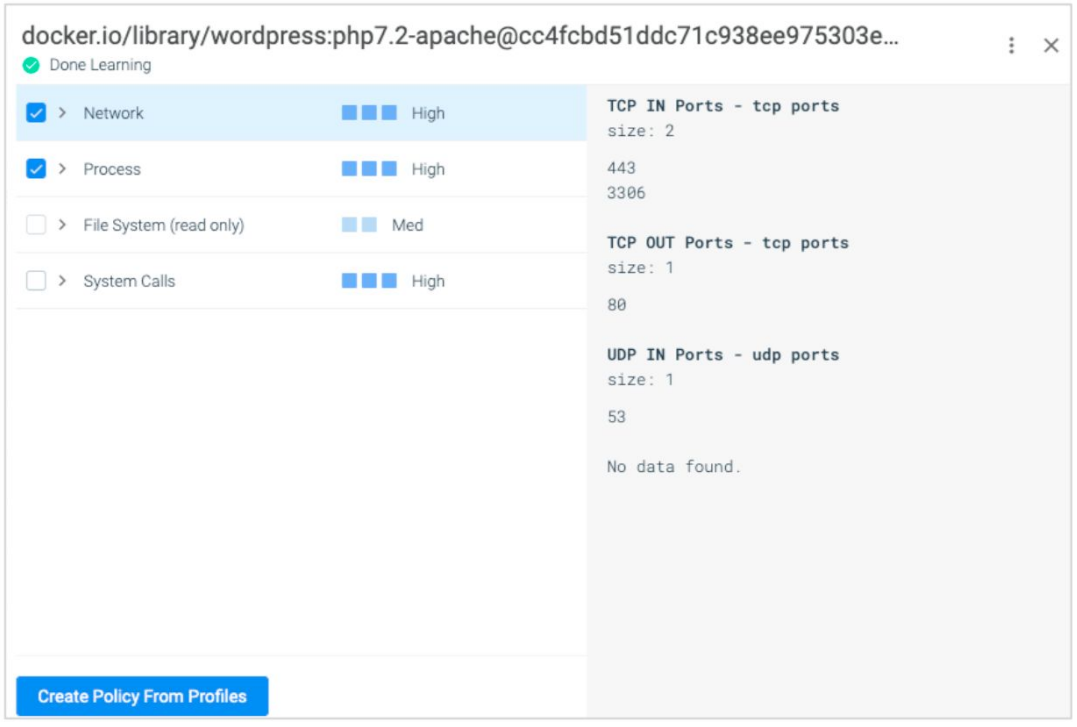
コンテナコンプライアンスアプローチ

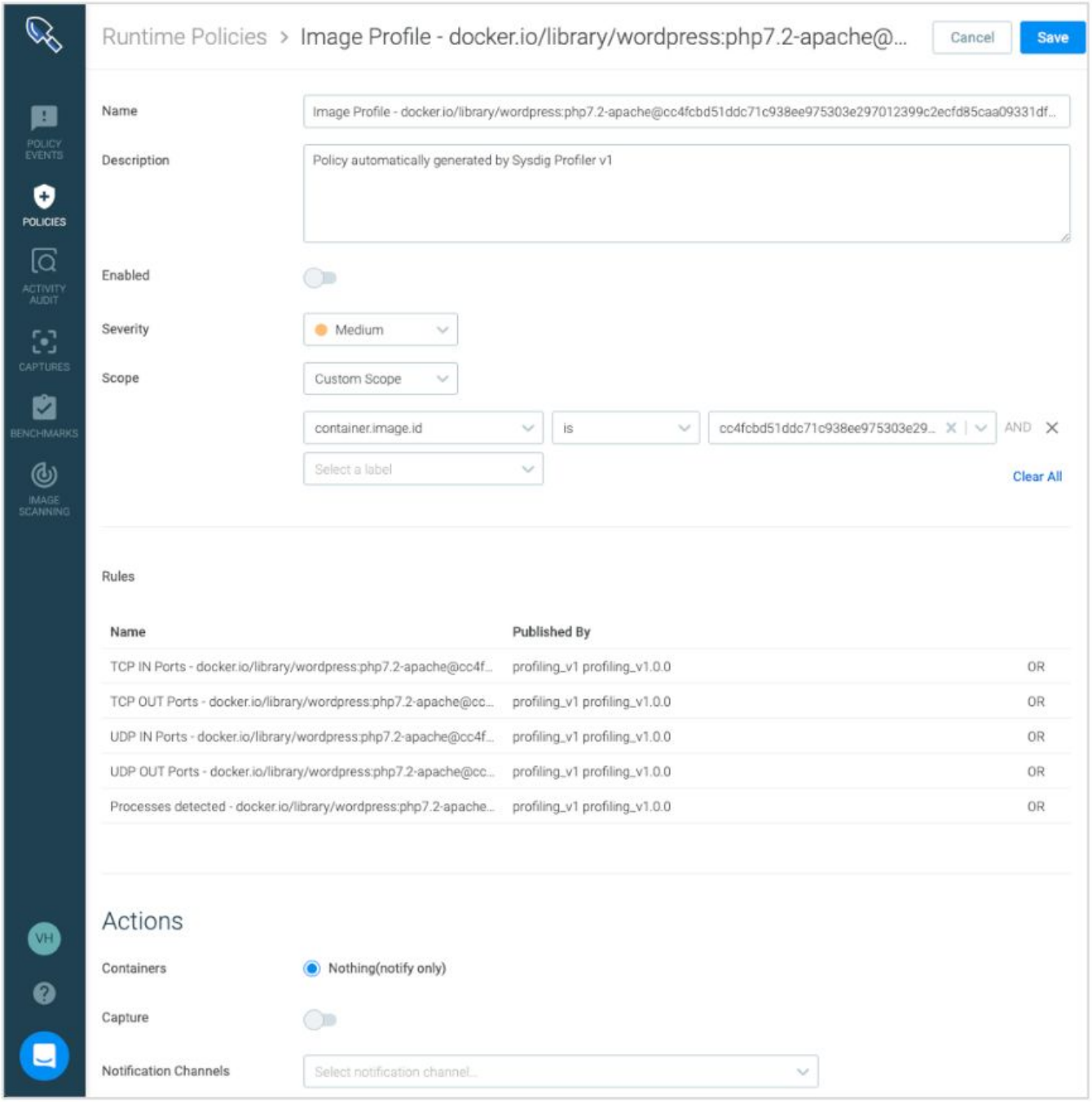
コンテナは、可能な限り分離してアプリケーションを設計する機会を提供します。これは、コンテナごとに1つのプロセスを実行し、インフラストラクチャ内のどこでも同じネットワークおよびファイルパターンで標準ポートを介して通信することを意味します。

Sysdigがどのように役立つか

Sysdigは、環境内のすべてのアクティビティを調べて、システム動作のベースラインを作成します。そこから、ポリシーを自動生成し、コンテナで実行中の予期しないプロトコル、デーモン、プロセスなどがあるかどうかを簡単に検出できます。


POLICIES
Image Profiles BETA
All Statuses
High Confidence
Confidence Levels
Status
Image
Network
Processes
File System
System Calls
docker.io/library/wordpress:php7.2-apache@cc4fcbd51ddc
docker.io/sysdiglabs/recurling:0.2@3945d89e4694
registry.ng.bluemix.net/armada-master/haproxy:9fad212615fd80337b9a6489d5c48581025ff421@30078938790c
registry.ng.bluemix.net/armada-master/node:v3.6.5@9b23e1a2ef6d
docker.io/sysdig/agent:9.5.0@a8e14ccb19ce
602401143452.dkr.ecr.us-east-1.amazonaws.com/eks/pause-amd64:3.1@9e462c010bf3
mysql:5.7@383867b75fd2
k8s.gcr.io/coredns:1.3.1@eb516548c180
weaveworks/weave-npc:2.5.1@789b7f496034
k8s.gcr.io/kube-proxy:v1.14.0@5cd54e388aba
registry.ng.bluemix.net/armada-master/keepalived-watcher:169@2a8075db8a57
registry.ng.bluemix.net/armada-master/storage-file-plugin:357@53ab40d4f5f4


docker.io/library/wordpress:php7.2-apache@cc4fcbd51ddc71c938ee975303e...
Done Learning
Network
High
Process
High
File System (read only)
Med
System Calls
High
TCP IN Ports - tcp ports
size: 2
443
3306
TCP OUT Ports - tcp ports
size: 1
80
UDP IN Ports - udp ports
size: 1
53
No data found.
Create Policy From Profiles



また、Falcoルールを使用して、2.2.1で説明されているように、指定されたバイナリとポートの外部の接続を検出することもできます。

2.4システムコンポーネントのインベントリ

要件の説明

PCI DSSの範囲内にあるシステムコンポーネントのインベントリを維持します。

ガイドライン

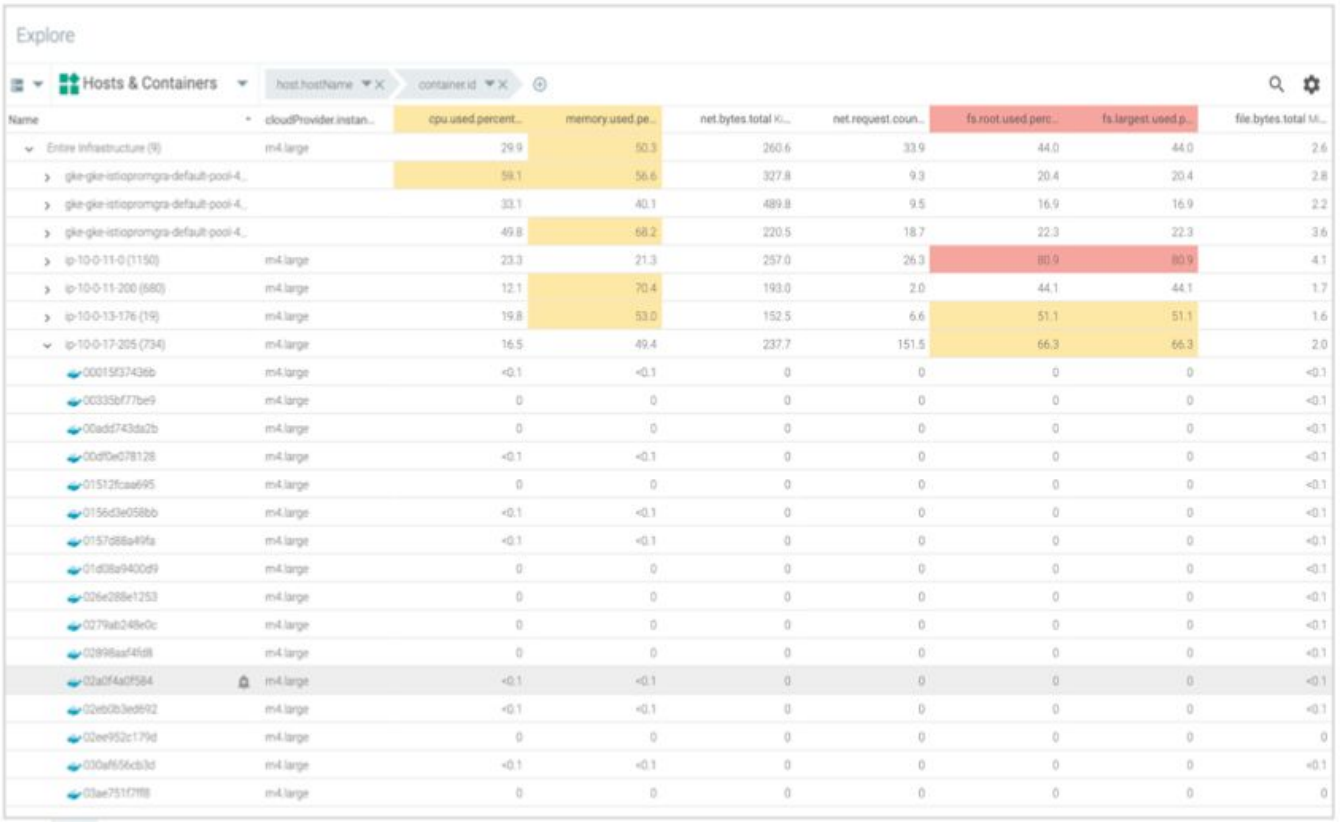
すべてのシステムコンポーネントの最新リストを維持することにより、組織はPCI DSSコントロールを実装するための環境の範囲を正確かつ効率的に定義できます。インベントリがないと、一部のシステムコンポーネントが忘れられ、組織の構成標準から誤って除外される可能性があります。

コンテナコンプライアンスアプローチ

多くの場合、コンテナはオーケストレーターでデプロイされます。これは、どのコンテナがどこでデプロイされているかを個人が制御できなくなったことを意味します。また、コンテナが環境に導入される速度増してくるため、強力なコンプライアンスを維持するには、現在実行されていることと過去に実行されたことを十分に理解する必要があります。

Sysdigがどのように役立つか

Sysdigには、システム上で実行されているすべてのホストとコンテナの全体的なビューをユーザーに提供するエクスプローラビューが付属しています。このテーブルを使用して、選択したすべてのシステムコンポーネントをスライスおよびダイスできます。表の下部にある時間コントロールを使用することにより、ユーザーはいつでも特定の物理インフラストラクチャで実行されているコンテナを常に確認できます。


Explore
Hosts & Containers
host.hostName
container.id
Name
cloudProvider.instan...
cpu.used.percent...
memory.used.pe...
Entire Infrastructure (9)
m4.large
29.9
50.3
gke-gke-istiopromgra-default-pool-4...
59.1
56.6
gke-gke-istiopromgra-default-pool-4...
33.1
40.1
gke-gke-istiopromgra-default-pool-4...
49.8
68.2
ip-10-0-11-0 (1150)
m4.large
23.3
21.3
ip-10-0-11-200 (680)
m4.large
12.1
70.4
ip-10-0-13-176 (19)
m4.large
19.8
53.0
ip-10-0-17-205 (734)
m4.large
16.5
49.4
00015f37436b
m4.large
<0.1
<0.1
00335bf77be9
m4.large
0
0

2.6 共有ホスティング分離保護

要件の説明

共有ホスティングプロバイダーは、各エンティティのホスト環境とカード会員データを保護する必要があります。

ガイドライン

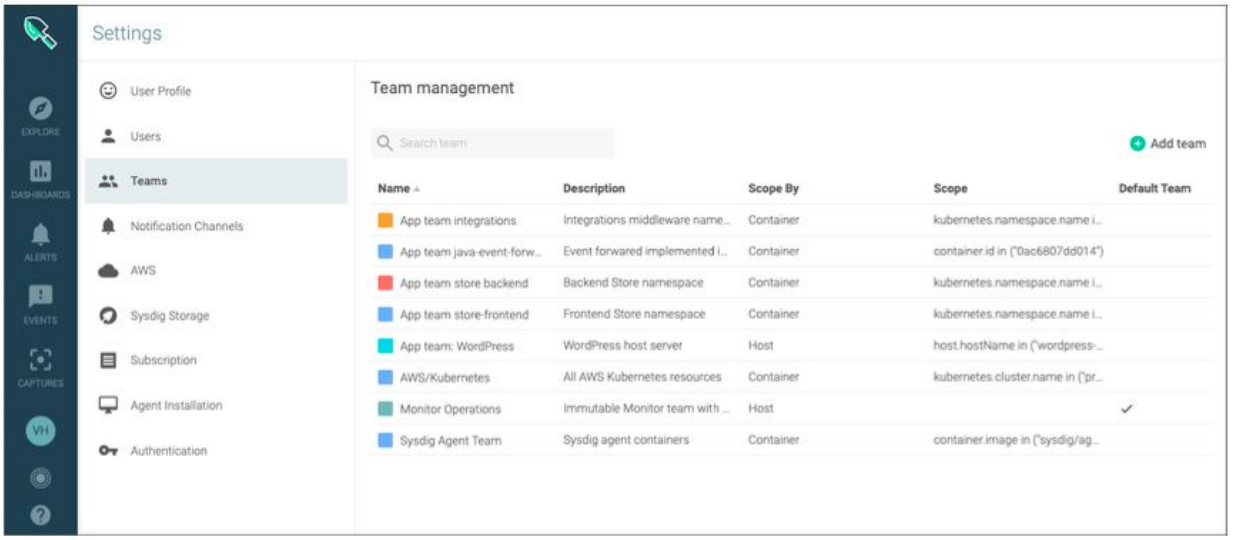
これは、同じサーバー上の複数のクライアントに共有ホスティング環境を提供するホスティングプロバイダー向けです。すべてのデータが同じサーバー上にあり、単一の環境の制御下にある場合、これらの共有サーバーの設定は通常、個々のクライアントで管理できません。これにより、クライアントは他のすべてのクライアント環境のセキュリティに影響する安全でない機能とスクリプトを追加できるため、悪意のある個人が他のすべてのクライアントのデータにアクセスして、あるクライアントのデータを簡単に侵害することができます。

コンテナコンプライアンスアプローチ

コンテナの最大の利点の1つは、同じ物理インフラストラクチャで複数のワークロードを実行することにより、リソース消費を削減できることです。これにより、データをセグメント化し、ユーザーにマルチテナント機能を提供する機能が複雑になりました。

Sysdigがどのように役立つか

Sysdigのチーム機能は、コンテナ環境から収集したパフォーマンス監視データへのアクセスをセグメント化するために使用されます。金融取引およびホスティングの顧客は、これを使用して、顧客に環境全体へのアクセスを許可せずに顧客にデータを提供できます。また、これはデータのアクセスを許可せずに、開発者がインターナルでサービスがどのように提供されているのかを把握する用途で使用することもできます。



Falcoランタイムセキュリティルールは、ユーザーまたはバイナリがスレッドネーススペースを変更したかどうかを検出できます。

```
# This list allows for easy additions to the set of commands allowed

# to change thread namespace without having to copy and override the

# entire change thread namespace rule.

- list: user_known_change_thread_namespace_binaries

  items: []

- macro: user_known_change_thread_namespace_activities

  condition: (never_true)

- list: network_plugin_binaries

  items: [aws-cni, azure-vnet]
```

```
- macro: calico_node
  condition: (container.image.repository endswith calico/node and proc.name=calico-node)
- macro: weaveworks_scope
  condition: (container.image.repository endswith weaveworks/scope and proc.name=scope)
- rule: Change thread namespace
  desc: >
    an attempt to change a program/thread\'s namespace (commonly done
    as a part of creating a container) by calling setns.
  condition: >
    evt.type = setns
    and not proc.name in (docker_binaries, k8s_binaries, lxd_binaries, sysdigcloud_binaries,
                          sysdig, nsenter, calico, oci-umount, network_plugin_binaries)
    and not proc.name in (user_known_change_thread_namespace_binaries)
    and not proc.name startswith "runc"
    and not proc.cmdline startswith "containerd"
    and not proc.pname in (sysdigcloud_binaries)
    and not python_running_sdchecks
    and not java_running_sdjagent
    and not kubelet_running_loopback
    and not rancher_agent
    and not rancher_network_manager
    and not calico_node
```

```
    and not weaveworks_scope
    and not user_known_change_thread_namespace_activities
  output: >
    Namespace change (setns) by unexpected program (user=%user.name command=%proc.cmdline
    parent=%proc.pname %container.info container_id=%container.id
    image=%container.image.repository)
  priority: NOTICE
  tags: [process, PCI, PCI_DSS_6.4.2]
```

Falcoランタイムセキュリティルールは、インバウンドネットワークトラフィックが、隔離する必要があるコンテナのローカルエリアネットワークの外部から来る場合を検出できます。

```
# Rule to detect network connection outside local subnet
- macro: enabled_rule_network_only_subnet
  condition: never_true
- list: images_allow_network_outside_subnet
  items: []
- macro: scope_network_only_subnet
  condition: >
    not container.image.repository in (images_allow_network_outside_subnet)
- macro: network_local_subnet
```

```
  condition: >
    fd.rnet in (rfc_1918_addresses) or
    fd.ip = "0.0.0.0" or
    fd.net = "127.0.0.0/8"
- rule: Network connection outside local subnet
  desc: Scoped images should only receive and send traffic to local subnet
  condition: >
    enabled_rule_network_only_subnet and
    inbound_outbound and
    container and
    not network_local_subnet and
    scope_network_only_subnet
  output: >
    Network connection outside local subnet
    (command=%proc.cmdline connection=%fd.name user=%user.name container_id=%container.id
    image=%container.image.repository namespace=%k8s.ns.name
    fd.rip.name=%fd.rip.name fd.lip.name=%fd.lip.name fd.cip.name=%fd.cip.name
    fd.sip.name=%fd.sip.name)
  priority: WARNING
  tags: [network, PCI, PCI_DSS_6.4.2]
```

要件4：

オープンなパブリックネットワークを介したカード会員データの送信を暗号化する

機密情報は、悪意のある個人が簡単にアクセスできるネットワークを介したやりとりにおいて暗号化する必要があります。誤った設定のワイヤレスネットワーク、レガシー暗号化および認証プロトコルの脆弱性は、脆弱性を悪用してカード会員データ環境への特権アクセスを取得する悪意のある個人の標的となります。

4.0 機密データ用の強力な暗号化

要件

強力な暗号化とセキュリティプロトコルを使用して、オープンなパブリックネットワークを介した送信中に、次のようなカード所有者の機密データを保護します。

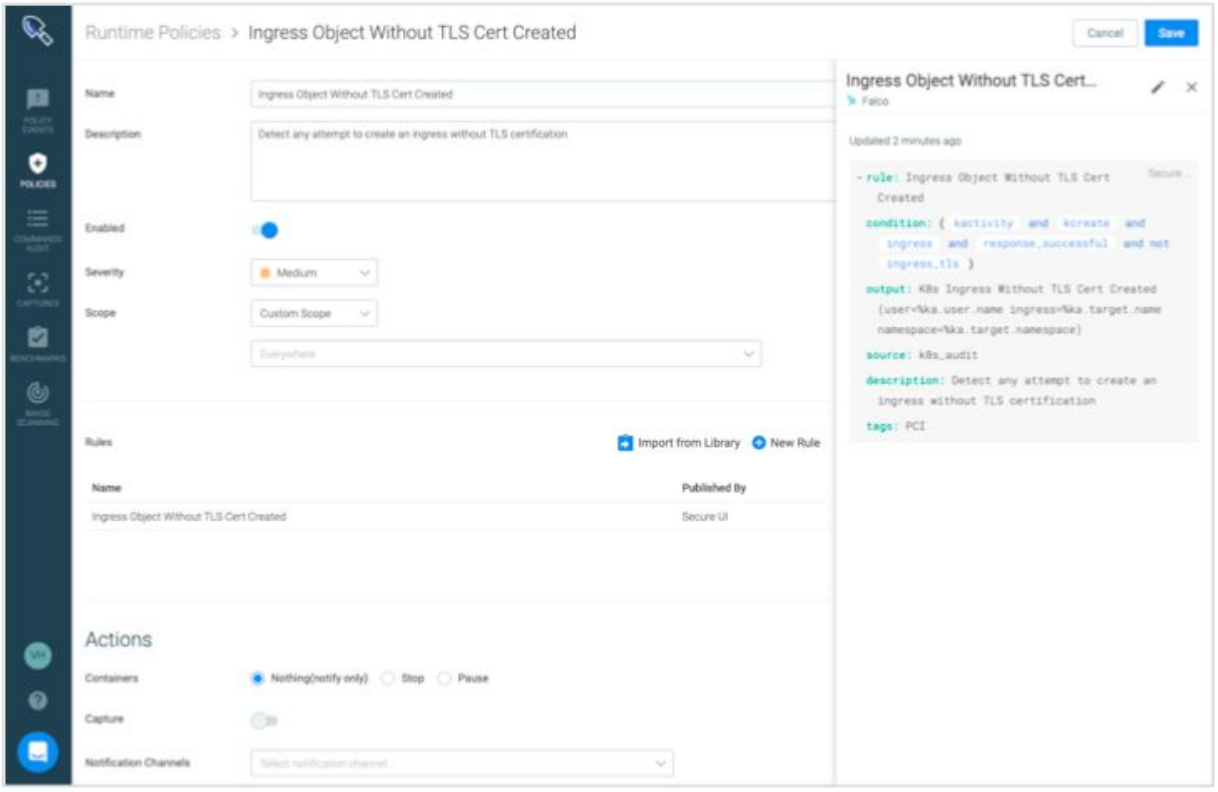
- 信頼できるキーと証明書のみが受け入れる
- 使用中のプロトコルは、安全なバージョンまたは構成のみをサポート
- 暗号化強度は、暗号化メソとロジーとして使われている物に適合している。 オープンなパブリックネットワークを介したカード会員データの送信を暗号化

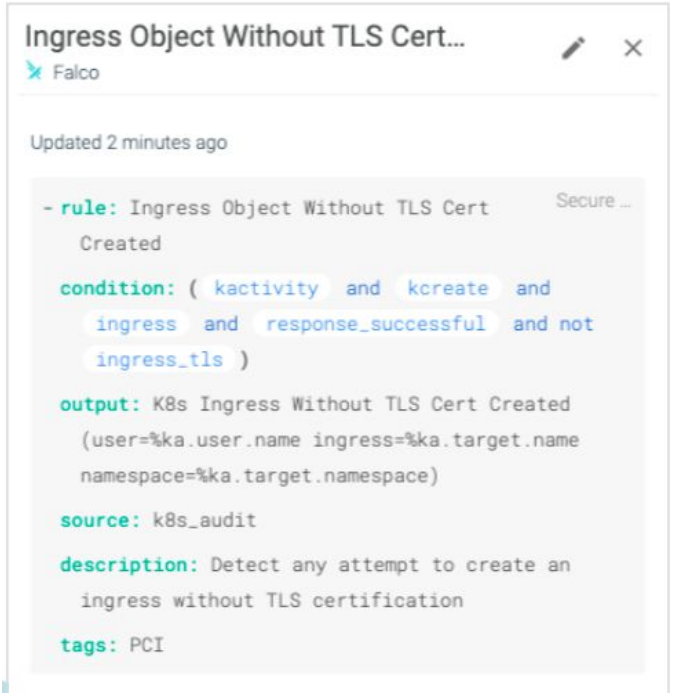
ガイドライン

この要件の目的は、コンテナ化されたアプリケーションまたはサービスが安全に通信しているかどうかを組織が検出できることです。

Sysdigの機能

Sysdigは、たとえばSSL / TLSを使用しない暗号化されていない接続を検出し、自動的にアラートをトリガーできます。


Runtime Policies > Ingress Object Without TLS Cert Created
Cancel
Save
Name
Ingress Object Without TLS Cert Created
Description
Detect any attempt to create an ingress without TLS certification
Enabled
Severity
Medium
Scope
Custom Scope
Everywhere
Rules
Import from Library
New Rule
Name
Published By
Ingress Object Without TLS Cert Created
Secure UI
Actions
Containers
Nothing(notify only)
Stop
Pause
Capture
Notification Channels
Ingress Object Without TLS Cert...
Falco
Updated 2 minutes ago
- rule: Ingress Object Without TLS Cert Created
condition: (kactivity and kcreate and ingress and response_successful and not ingress_tls)
output: K8s Ingress Without TLS Cert Created (user=%ka.user.name ingress=%ka.target.name namespace=%ka.target.namespace)
source: k8s_audit
description: Detect any attempt to create an ingress without TLS certification
tags: PCI


Ingress Object Without TLS Cert...
Falco
Updated 2 minutes ago
Secure ...
- rule: Ingress Object Without TLS Cert Created
condition: (kactivity and kcreate and ingress and response_successful and not ingress_tls)
output: K8s Ingress Without TLS Cert Created (user=%ka.user.name ingress=%ka.target.name namespace=%ka.target.namespace)
source: k8s_audit
description: Detect any attempt to create an ingress without TLS certification
tags: PCI

TLS証明書なしでKubernetesクラスター内のイングレスオブジェクトの作成を検出するFalcoルール

```
# Applies to standard:
# PCI 4.0. Strong cryptography for sensitive data
- macro: kactivity
  condition: (kevt and consider_activity_events)
- macro: kcreate
  condition: ka.verb=create
- macro: response_successful
  condition: (ka.response.code startswith 2)
- macro: ingress
  condition: ka.target.resource=ingresses
- macro: ingress_tls
  condition: (jevt.value[/requestObject/spec/tls] exists)
- rule: Ingress Object Without TLS Cert Created
  desc: Detect any attempt to create an ingress without TLS certification
  condition: >
    (kactivity and kcreate and ingress and response_successful and not ingress_tls)
  output: >
    K8s Ingress Without TLS Cert Created (user=%ka.user.name ingress=%ka.target.name
    namespace=%ka.target.namespace)
  source: k8s_audit
  priority: WARNING
  tags: [k8s, network, PCI, PCI_DSS_4.0]
```

要件6：

安全なシステムとアプリケーションの開発と維持

6.1 ランキングによるセキュリティ脆弱性の特定

要件の説明

セキュリティ脆弱性情報の信頼できる外部ソースを使用して、セキュリティ脆弱性を識別するプロセスを確立し、新たに発見されたセキュリティ脆弱性にリスクランキング（「高」、「中」、「低」など）を割り当てます。

ガイドライン

この要件の目的は、組織が環境に影響を与える可能性のある新しい脆弱性を最新の状態に保つことです。

脆弱性情報のソースは信頼できるものでなければならず、多くの場合、ベンダーのWebサイト、業界ニュースグループ、メーリングリスト、またはRSSフィードが含まれます。

組織が環境に影響を与える可能性のある脆弱性を特定したら、脆弱性がもたらすリスクを評価してランク付けする必要があります。したがって、組織は、継続的に脆弱性を評価し、それらの脆弱性にリスクランキングを割り当てるための方法を用意する必要があります。これは、ASVスキャンまたは内部脆弱性スキャンでは達成されず、むしろ、脆弱性情報の業界ソースを積極的に監視するプロセスが必要です。

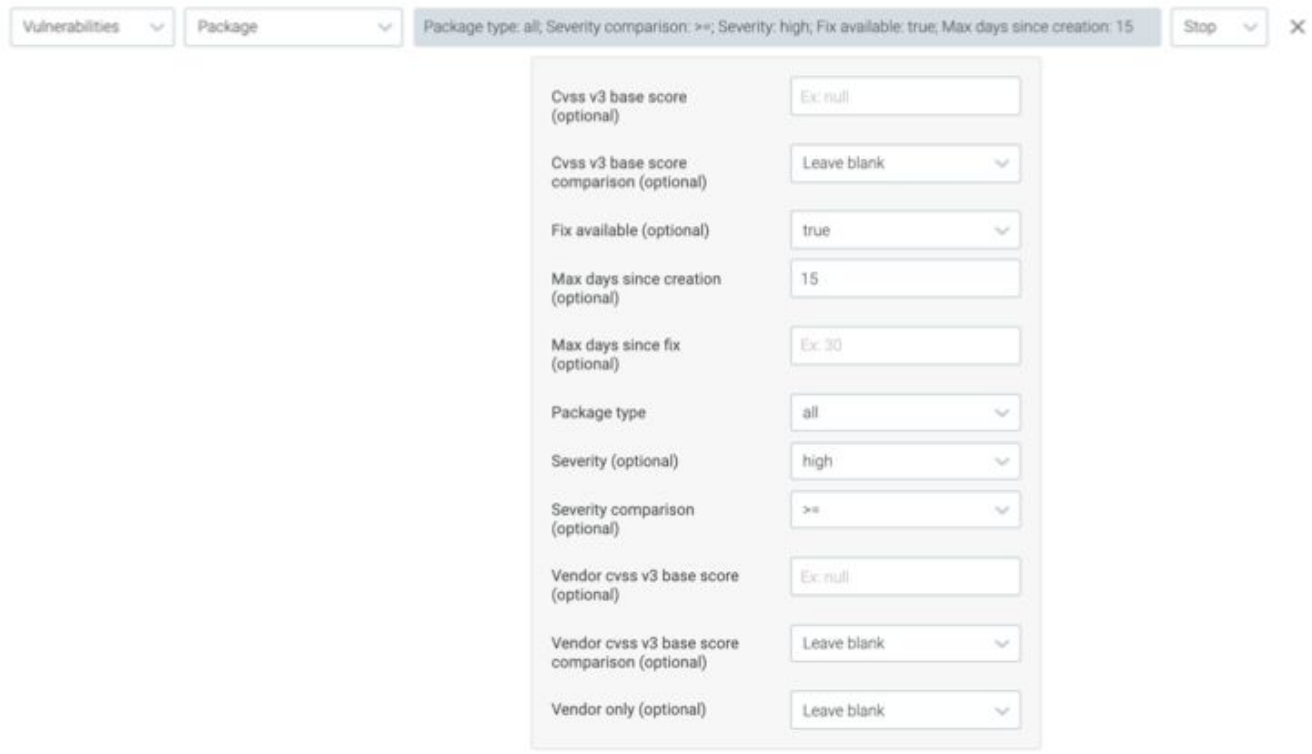
リスクを分類することで（たとえば、「高」、「中」、「低」など）、組織は最もリスクの高い項目をより迅速に特定、優先順位付け、対処し、最大のリスクをもたらす脆弱性が悪用される可能性を減らすことができます。

コンテナコンプライアンスアプローチ

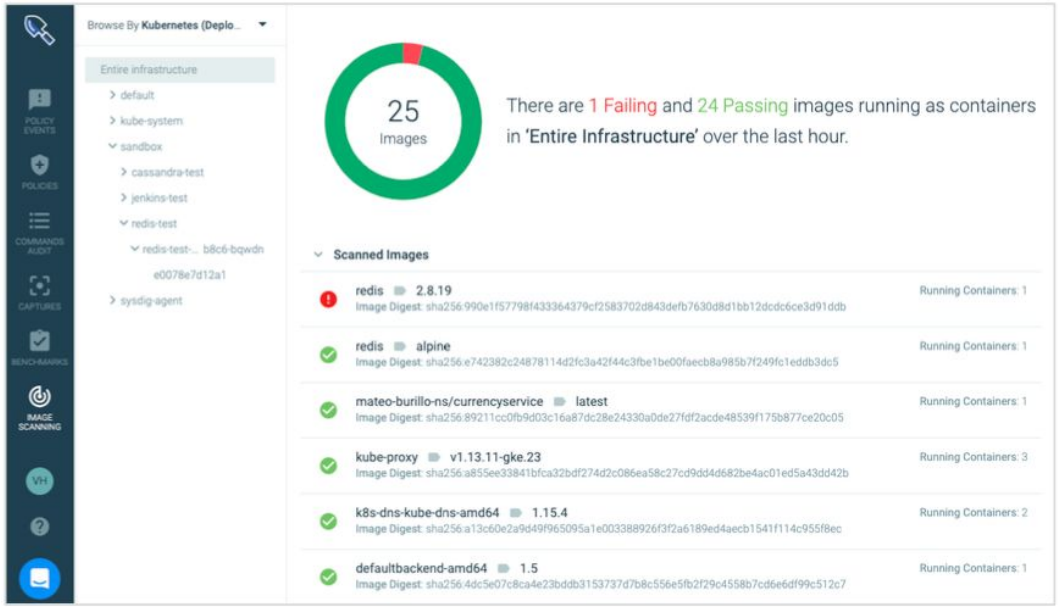
コンテナ化されたアプリケーションを従来のアプリケーションよりも速くCI/CDパイプラインを介して移動できるため、コンテナの脆弱性リスクを修正するのは簡単です。脆弱性の侵入を防ぐため、実稼働組織はレジストリ内でCI/CDプロセスの一部として脆弱性のイメージをスキャンし、実稼働コンテナの脆弱性を監視する必要があります。

Sysdigがどのように役立つか

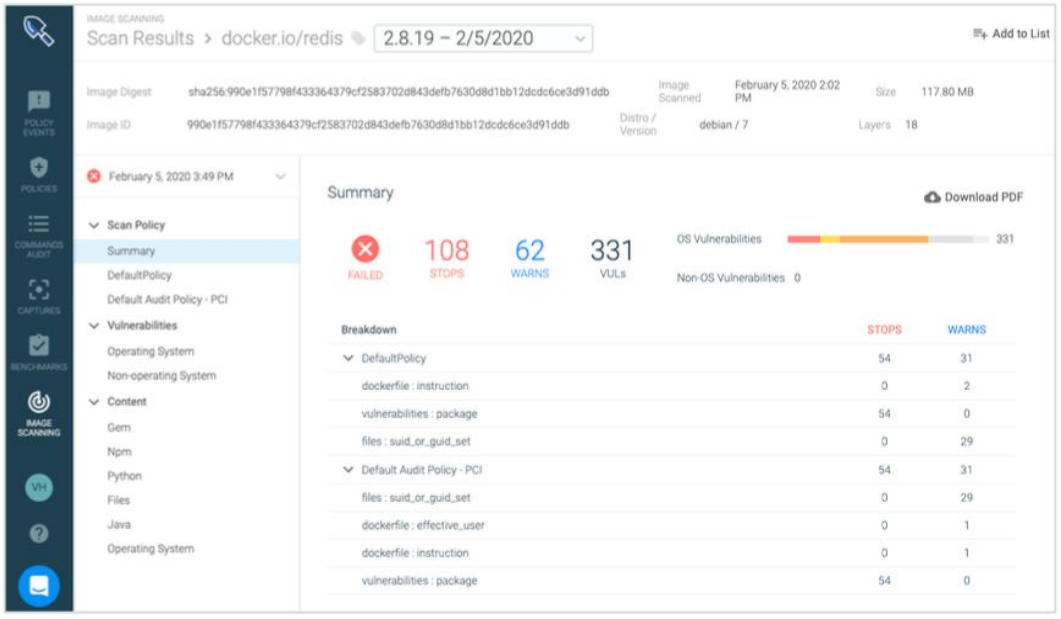
ビルド中のイメージに修正が必要な重大な脆弱性が含まれている場合、ビルドをフェイルさせるポリシーを簡単に定義できます。



セキュリティスキャンに失敗したコンテナを特定して、リスクを軽減する方法を見つけるためにドリルインします。



レポートを表示して、イメージがスキャン評価に失敗した理由を確認します。



6.2 ベンダーセキュリティパッチをインストールする

要件の説明

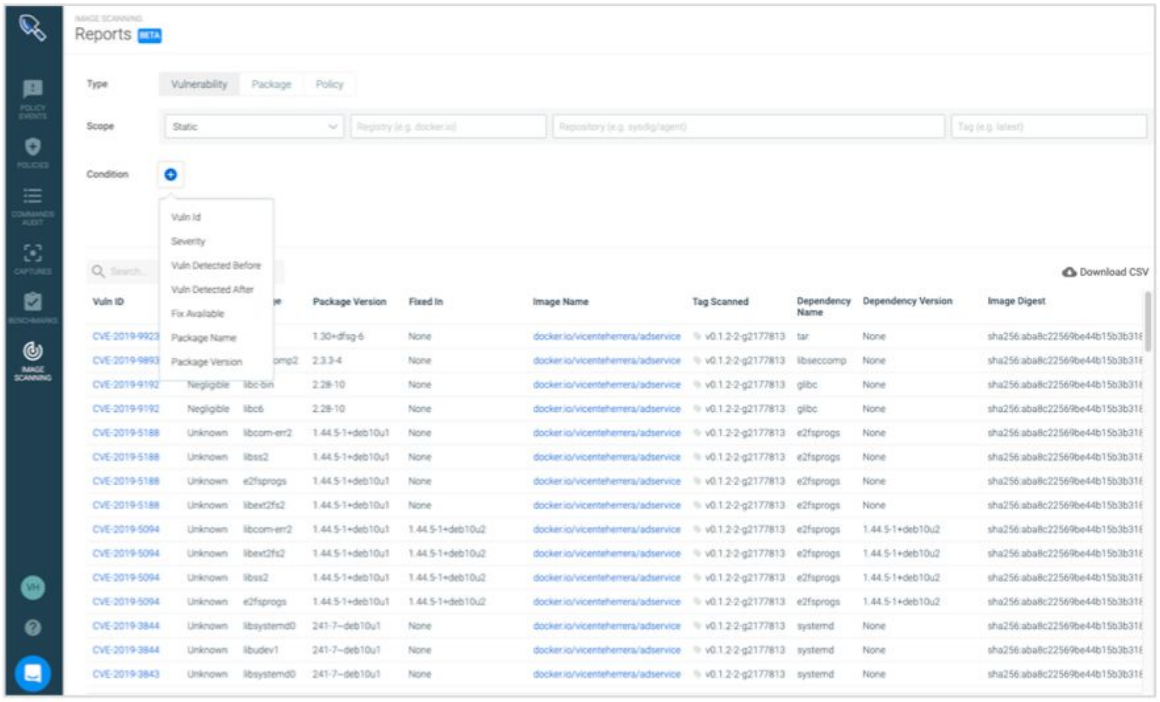
該当するベンダー提供のセキュリティパッチをインストールすることにより、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認してください。リリースから1か月以内に重要なセキュリティパッチをインストールします。

ガイドライン

多くの場合、アプリケーションセキュリティチームは、30日以内に修正を行って重大度の高いCVEに対処する必要があります。

Sysdigがどのように役立つか

Sysdig Secureを使用すると、従来のパッチ管理プロセスをコンテナーに組み込むことができます。チームは、レジストリで、および/または特定のネームスペース、クラスター、クラウドリージョンで実行されている脆弱性レポートのポリシーを設定できます。その後、CVE ID、重大度、fix、age、またはその他の基準などの高度な条件によって特定の脆弱性を照会できます。



CVE-2019-5188	Unknown	libss2	1.44.5-1+deb10u1	None	docker.io/vicenteherrera/adservice
CVE-2019-5188	Unknown	e2fsprogs	1.44.5-1+deb10u1	None	docker.io/vicenteherrera/adservice
CVE-2019-5188	Unknown	libext2fs2	1.44.5-1+deb10u1	None	docker.io/vicenteherrera/adservice
CVE-2019-5094	Unknown	libcom-err2	1.44.5-1+deb10u1	1.44.5-1+deb10u2	docker.io/vicenteherrera/adservice
CVE-2019-5094	Unknown	libext2fs2	1.44.5-1+deb10u1	1.44.5-1+deb10u2	docker.io/vicenteherrera/adservice
CVE-2019-5094	Unknown	libss2	1.44.5-1+deb10u1	1.44.5-1+deb10u2	docker.io/vicenteherrera/adservice
CVE-2019-5094	Unknown	e2fsprogs	1.44.5-1+deb10u1	1.44.5-1+deb10u2	docker.io/vicenteherrera/adservice

6.3 PCI DSSに準拠しベストプラクティスを開発する

要件の説明

次のように、内部および外部ソフトウェアアプリケーション（アプリケーションへのWebベースの管理アクセスを含む）を安全に開発します。

- PCI DSSに準拠（安全な認証+ロギングなど）
- 業界標準および/またはベストプラクティスに基づく
- ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込む

ガイドライン

ソフトウェア開発の要件定義、設計、分析、およびテストの段階でセキュリティを含めないと、セキュリティの脆弱性が不注意または悪意で本番環境に導入される可能性があります。

Sysdigがどのように役立つか

Sysdigにはネイティブのjenkinsプラグインがあり、Bamboo、Gitlab、CircleCIなどのツールと統合して、イメージスキャンをソフトウェア開発プロセスに簡単に統合できます。このスキャンは、脆弱性、公開されたポート、古いパッケージ、およびセキュリティのベストプラクティスに従わないその他のイメージコンテンツの特定に役立ちます。

6.4.2 開発/テスト本番環境を分離

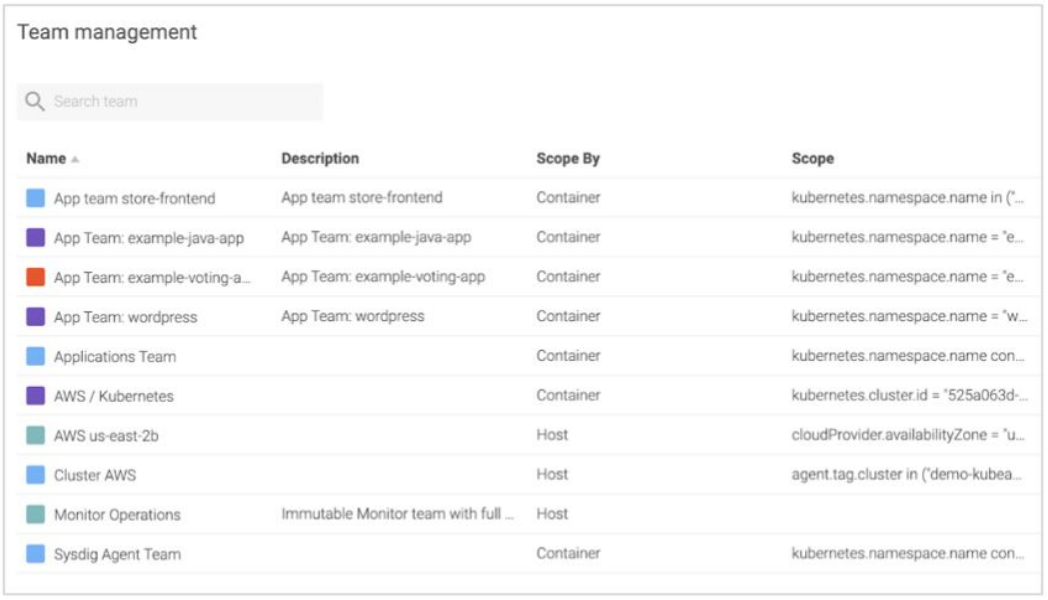
要件の説明

開発/テスト環境と本番環境で業務を分離。

Sysdigがどのように役立つか

Sysdigのチーム機能を使用して、開発/テスト環境などのさまざまなコンテナ環境へのアクセスをセグメント化できます。Sysdigは、開発環境、テスト環境、および本番環境でセグメント化されたコ

ンテナ化環境とKubernetes環境間のポリシーの分離をサポートしています。 環境は、ネームスペース、イメージ、ホスト、コンテナなどによって範囲を限定できます。



Kubernetesユーザーを却下するFalcoルール

```
# Generally only consider audit events once the response has completed
- list: k8s_audit_stages
  items: ["ResponseComplete"]
# Generally exclude users starting with "system:"
- macro: non_system_user
  condition: (not ka.user.name startswith "system:")
# This macro selects the set of Audit Events used by the below rules.
```

```
- macro: kevt
  condition: (jevt.value[/stage] in (k8s_audit_stages))
- macro: kevt_started
  condition: (jevt.value[/stage]=ResponseStarted)
# If you wish to restrict activity to a specific set of users, override/append to this list.
# users created by kops are included
- list: allowed_k8s_users
  items: ["minikube", "minikube-user", "kubelet", "kops", "admin", "kube", "kube-proxy"]
- rule: Disallowed K8s User
  desc: Detect any k8s operation by users outside of an allowed set of users.
  condition: kevt and non_system_user and not ka.user.name in (allowed_k8s_users)
  output: >
    K8s Operation performed by user not in allowed list of users
    (user=%ka.user.name target=%ka.target.name/%ka.target.resource verb=%ka.verb
    uri=%ka.uri resp=%ka.response.code)
  priority: WARNING
  source: k8s_audit
  tags: [k8s, PCI, PCI_DSS_6.4.2]
```

ローカルネットワークの外部からコンテナへの接続を検出するFalcoルール

```
# Rule to detect network connection outside local subnet

- macro: enabled_rule_network_only_subnet

  condition: never_true

- list: images_allow_network_outside_subnet

  items: []

- macro: scope_network_only_subnet

  condition: >

    not container.image.repository in (images_allow_network_outside_subnet)

- macro: network_local_subnet

  condition: >

    fd.rnet in (rfc_1918_addresses) or

    fd.ip = "0.0.0.0" or

    fd.net = "127.0.0.0/8"

- rule: Network connection outside local subnet

  desc: Scoped images should only receive and send traffic to local subnet

  condition: >

    enabled_rule_network_only_subnet and

    inbound_outbound and

    container and
```

```
    not network_local_subnet and
    scope_network_only_subnet
output: >
    Network connection outside local subnet
    (command=%proc.cmdline connection=%fd.name user=%user.name container_id=%container.id
    image=%container.image.repository namespace=%k8s.ns.name
    fd.rip.name=%fd.rip.name fd.lip.name=%fd.lip.name fd.cip.name=%fd.cip.name
    fd.sip.name=%fd.sip.name)
 priority: WARNING
 tags: [network, PCI, PCI_DSS_6.4.2]
```

6.5.1 SQLインジェクションなどの欠陥を検査する

要件の説明

インジェクションの欠陥、特にSQLインジェクション。また、OSコマンドインジェクション、LDAPおよびXPathインジェクションの欠陥、およびその他のインジェクションの欠陥も考慮してください。

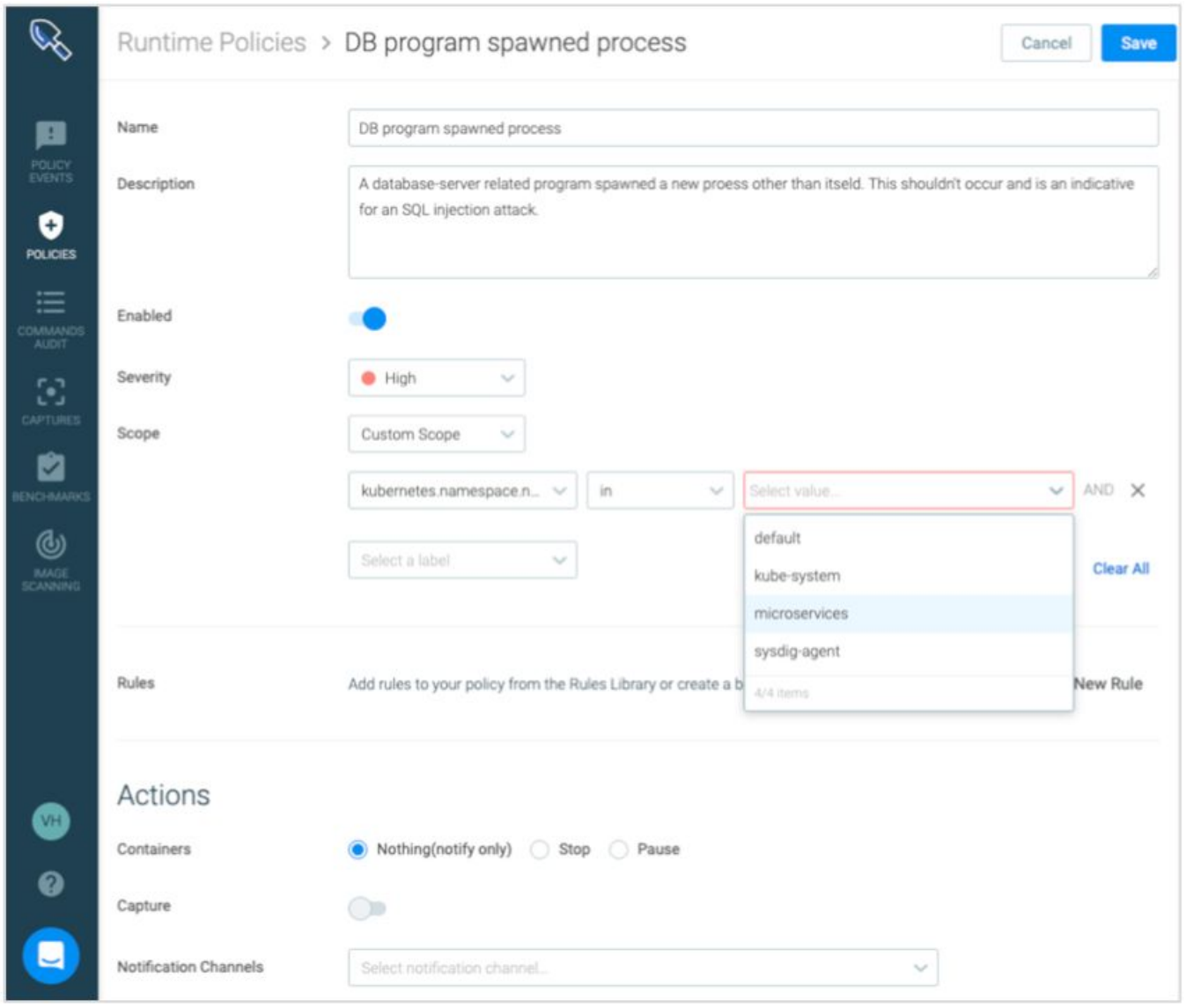
ガイドライン

インジェクションの欠陥、特にSQLインジェクションは、アプリケーションを侵害するためによく使用される方法です。インジェクションは、ユーザーが指定したデータがコマンドまたはクエリの一部としてインタープリターに送信されるときに発生します。攻撃者の敵意のあるデータは、インタープリターに意図しないコマンドの実行やデータの変更をさせます。これにより、攻撃者はアプリケーションを介してネットワーク内のコンポーネントを攻撃し、バッファオーバーフローなどの攻撃を開始したり、機密情報とサーバーアプリケーションの両方の機能を明らかにしたりできます。

Sysdigがどのように役立つか

Sysdigは、システムから来る根本的に悪意のある動作を探します。これは、標準的なインジェク

ションと侵入だけでなく、ユーザーがrpmパッケージを変更する、データベースからの予期しない動作、またはネットワークアクティビティのあるシステムバイナリを含む分類が難しい動作もカバーします。



DBプログラムがシェルプロセスを生成したことを検出するFalcoルール

```
- rule: DB program spawned process
  desc: >
    a database-server related program spawned a new process other than itself.
    This shouldn\'t occur and is a follow on from some SQL injection attacks.
  condition: >
    proc.pname in (db_server_binaries)
    and spawned_process
    and not proc.name in (db_server_binaries)
    and not postgres_running_wal_e
  output: >
    Database-related program spawned process other than itself
    (user=%user.name program=%proc.cmdline parent=%proc.pname container_id=%container.id
    image=%container.image.repository)
  priority: NOTICE
  tags: [process, database, mitre_execution, PCI, PCI_DSS_6.5.1]
```

6.5.6 高リスクの脆弱性

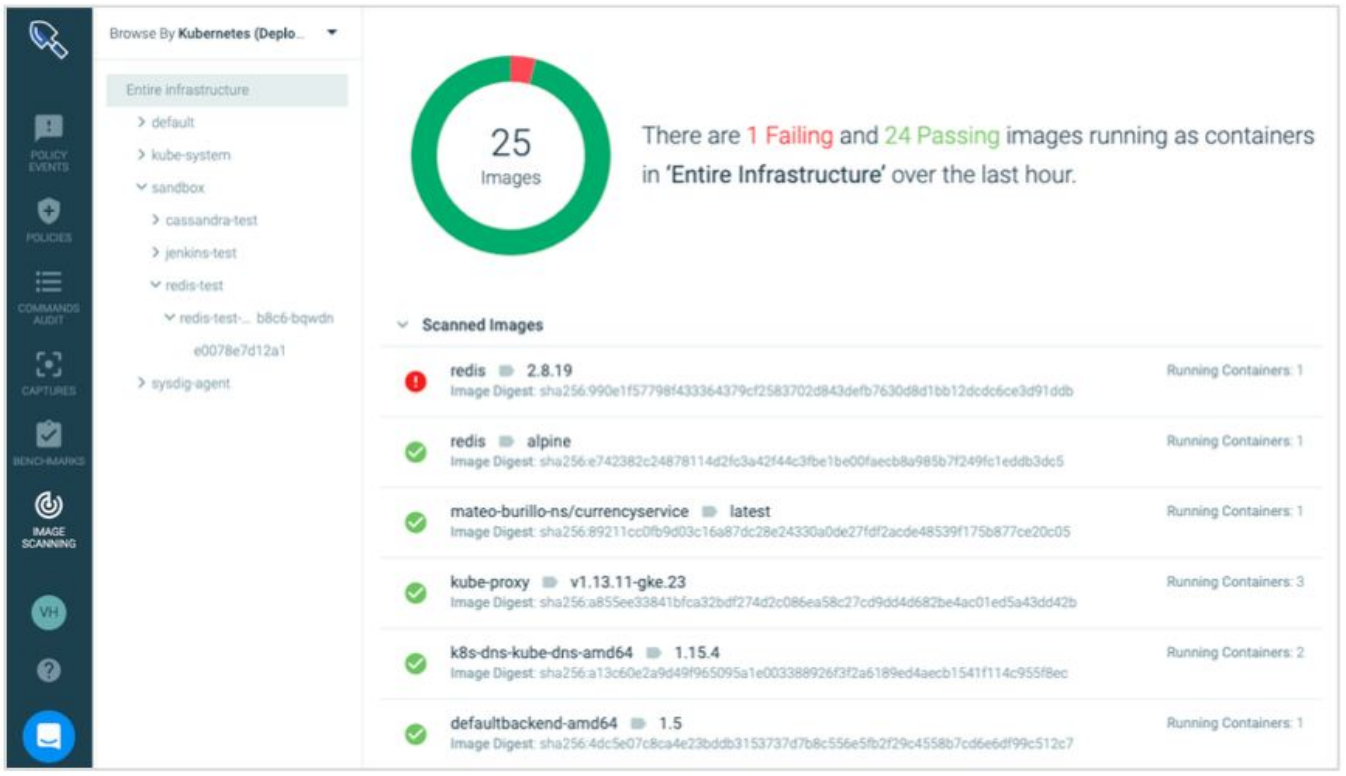
要件の説明

脆弱性識別プロセスで識別されたすべての「高リスク」脆弱性（PCI DSS要件6.1で定義）

Sysdigがどのように役立つか

Sysdigは、単一のワークフローで実行中のコンテナの脆弱性（CVE）および構成ミスを自動的にスキャンします。高リスクの脆弱性は、CVSSスコアに基づいてフラグが付けられ、実行時に特定のアプリケーション/ネームスペースにマップし直すことができます。これらの高リスクの脆弱性は、

スキャンポリシーをCI/CDパイプライン（例：Jenkins）に直接統合するか、Kubernetesのアドミッションコントローラーを介して防ぐことができます。



6.5.8 不適切なアクセス制御

安全でない直接オブジェクト参照、URLアクセスの制限の失敗、ディレクトリトラバーサル、機能へのユーザーアクセスの制限の失敗など、不適切なアクセス制御

要件の説明

ソフトウェア開発のポリシーと手順を調べ、責任者を面接して、不適切なアクセス制御（安全でない直接オブジェクト参照、URLアクセスの制限の失敗、ディレクトリトラバーサルなど）が以下を含むコーディング手法で対処されていることを確認します。

- ユーザーの適切な認証
- 入力のサニタイズ
- 内部オブジェクト参照をユーザーに公開しない
- 不正な機能へのアクセスを許可しないユーザーインターフェイス

ガイドライン

開発者がファイル、ディレクトリ、データベースレコード、キーなどの内部実装オブジェクトへの参照をURLまたはフォームパラメーターとして公開すると、オブジェクトへの直接参照が発生します。 攻撃者はこれらの参照を操作して、許可なく他のオブジェクトにアクセスできます。

すべてのURLのプレゼンテーション層とビジネスロジックで一貫してアクセス制御を実施します。多くの場合、アプリケーションが機密機能を保護する唯一の方法は、許可されていないユーザーへのリンクまたはURLの表示を防止することです。攻撃者はこの脆弱性を利用して、これらのURLに直接アクセスすることにより、不正な操作にアクセスし、実行することができます。

攻撃者はWebサイトのディレクトリ構造を列挙およびナビゲート（ディレクトリトラバーサル）できるため、不正な情報にアクセスしたり、後で悪用するためにサイトの仕組みをさらに詳しく知ることができます。ユーザーインターフェイスが許可されていない機能へのアクセスを許可する場合、このアクセスにより、許可されていない個人が特権的な資格情報またはカード会員データへのアクセスを取得する可能性があります。機密リソースへの直接オブジェクト参照へのアクセスを許可されたユーザーのみに許可する必要があります。データリソースへのアクセスを制限すると、カード会員データが不正なリソースに提示されるのを防ぐのに役立ちます。

Sysdigがどのように役立つか

クラスターを管理するための匿名のリクエストがリジェクトされたかった事を検出するFalcoルール

```
# Corresponds to K8s CIS Benchmark, 1.1.1.

- rule: Anonymous Request Allowed

  desc: Detect any request made by the anonymous user that was allowed

  condition: >

    kevt and ka.user.name=system:anonymous and ka.auth.decision!=reject
    and not health_endpoint

  output: >
    Request by anonymous user allowed
    (user=%ka.user.name verb=%ka.verb uri=%ka.uri reason=%ka.auth.reason))

 priority: WARNING

 source: k8s_audit

 tags: [k8s, PCI, PCI_DSS_6.5.8]
```

6.6 少なくとも年に1回と変更後に一般向けWebをレビューする

要件の説明

一般向けのWebアプリケーションの場合、次のいずれかの方法で、新しい脅威と脆弱性に継続的に対処し、これらのアプリケーションが既知の攻撃から保護されるようにします。手動または自動化されたアプリケーションの脆弱性セキュリティ評価ツールまたは方法論を使用して、少なくとも年に一度および変更後に公開されているWebアプリケーションをレビューする。

ガイドライン

公開アプリケーションは攻撃者の主な標的であり、コーディングが不十分なWebアプリケーションは、攻撃者が機密データやシステムにアクセスするための簡単な方法を提供します。アプリケーションのレビューまたはWebアプリケーションファイアウォール導入の要件は、不十分なコーディ

ングまたはアプリケーション管理慣行による一般向けWebアプリケーションの侵害の数を減らすことを目的としています。

コンテナにおける課題

コンテナのエフェメラルな性質により、インフラストラクチャを毎年では無く、頻繁にスキャンする必要が生じます。この要件は、サービスの新しいバージョンがデプロイされるとすぐに満たされるか、スキャンが継続的に実行される必要があります。

Sysdigがどのように役立つか

Sysdigは、パブリック環境および内部環境で実行されているコンテナの継続的な監視を提供します。 Sysdigは、脆弱性のリスクステータスが組織で定義されたしきい値を超えた場合にリアルタイムのアラートを行う事ができます。

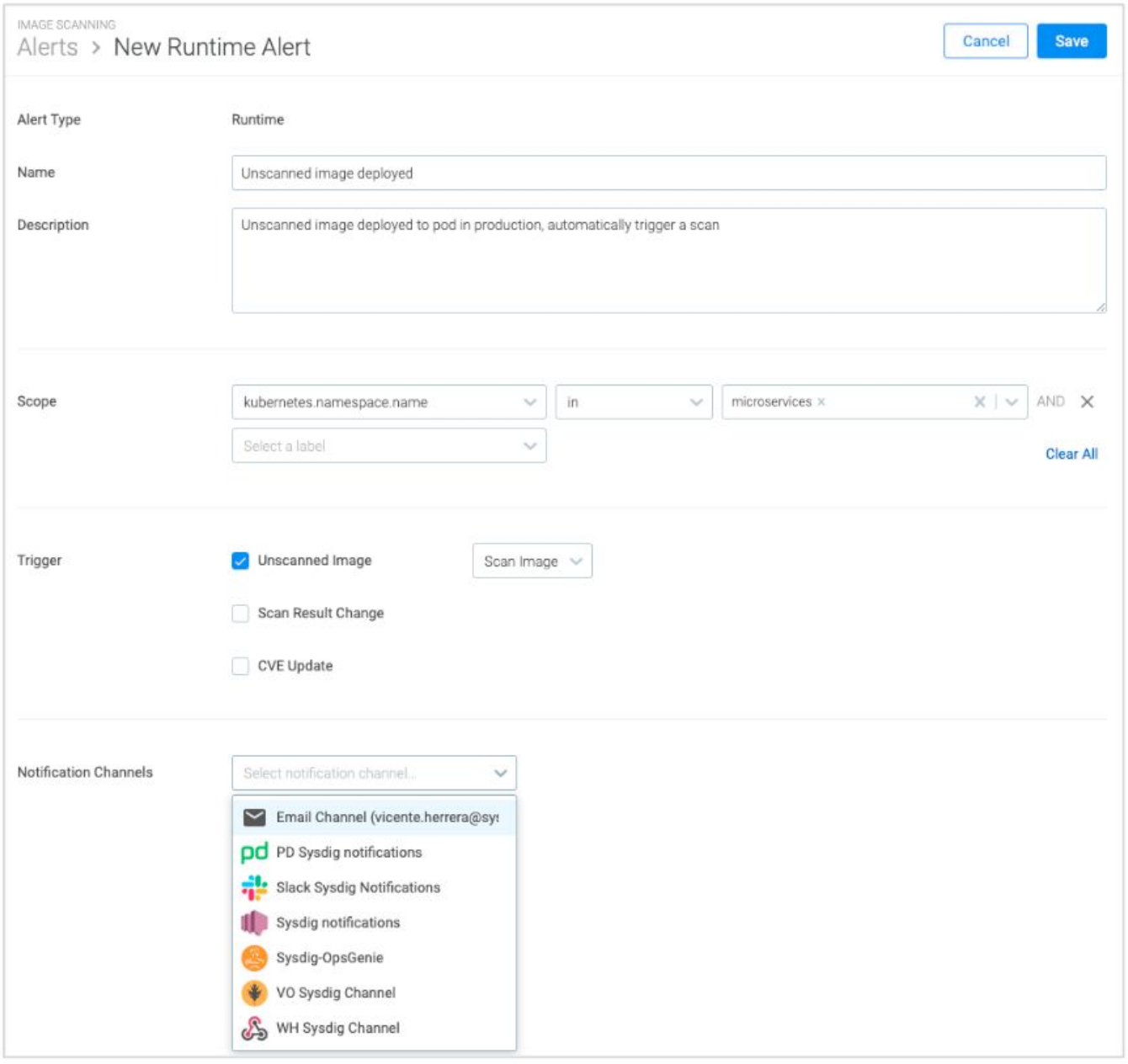


IMAGE SCANNING
Alerts > New Runtime Alert
Cancel
Save
Alert Type
Runtime
Name
Unscanned image deployed
Description
Unscanned image deployed to pod in production, automatically trigger a scan
Scope
kubernetes.namespace.name
in
microservices
AND
Select a label
Clear All
Trigger
Unscanned Image
Scan Image
Scan Result Change
CVE Update
Notification Channels
Select notification channel...
Email Channel (vicente.herrera@sy
PD Sysdig notifications
Slack Sysdig Notifications
Sysdig notifications
Sysdig-OpsGenie
VO Sysdig Channel
WH Sysdig Channel

要件7：

ビジネスによって必要とする場合のみに、カード会員データへのアクセスを制限する

重要なデータに権限のある人のみがアクセスできるようにするには、システムとプロセスを配備して、知る必要性と職責に基づいてアクセスを制限する必要があります。

7.1.2 特権ユーザーIDへのアクセスを制限する

要件の説明

特権ユーザーIDへのアクセスを、職責の実行に必要な最小限の特権に制限します。

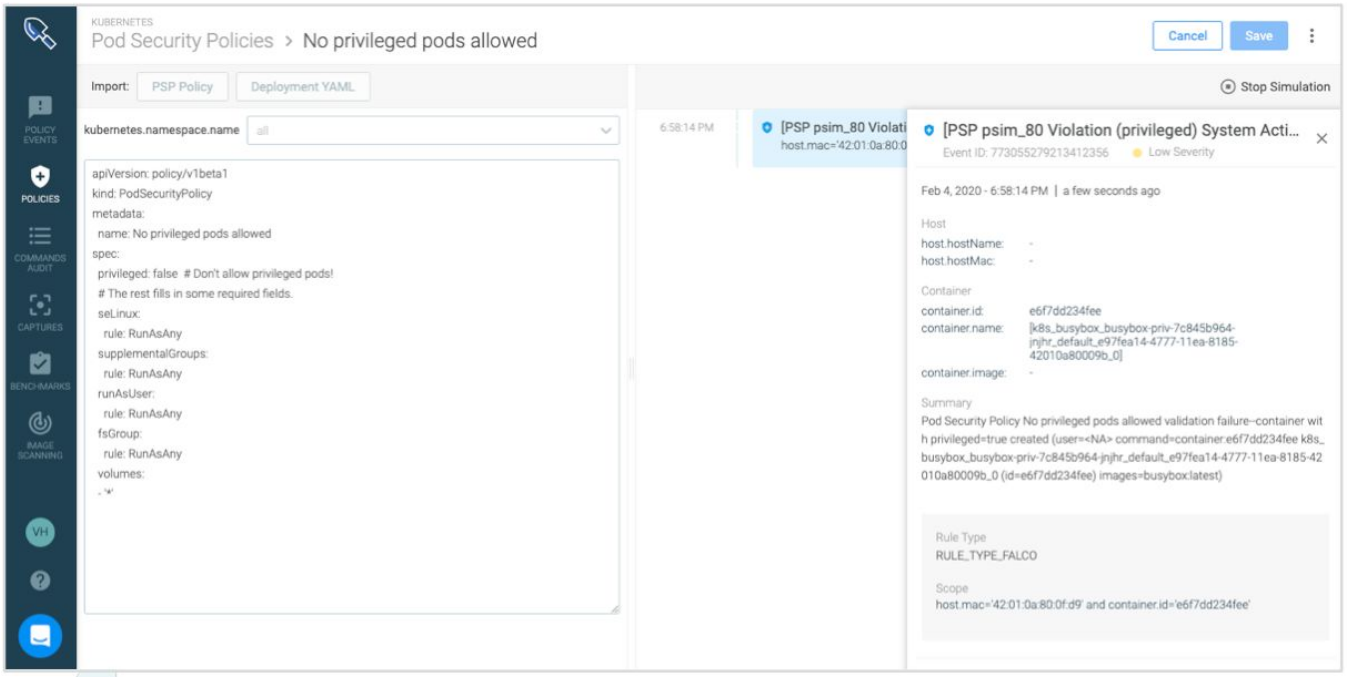
ガイドライン

ポッドセキュリティポリシーは、実質的には脅威防止メカニズムです。それらが実施するセキュリティ制約により、攻撃がクラスタ全体に広がるのを防ぎ、一般的なコンテナブレイクアウトアプローチをブロックします。PSPはAppArmor、SELinux、seccomp、またはLinux機能のようなきめ細かい実行時セキュリティプロファイルを適用することもできます。これにより、利用可能なルート特権のサブセットをプロセスに提供します。

Sysdigがどのように役立つか

Sysdigは、デプロイメント定義のPod仕様の要件を分析し、アプリケーションの最小特権PSPを作成します。これにより、特権ポッド、ユーザーがコンテナ、ボリュームなどとして実行できるようにするかどうかが制御されます。PSPを微調整し、デプロイメント前に検証するシミュレーションを

実行するネームスペースを定義できます。



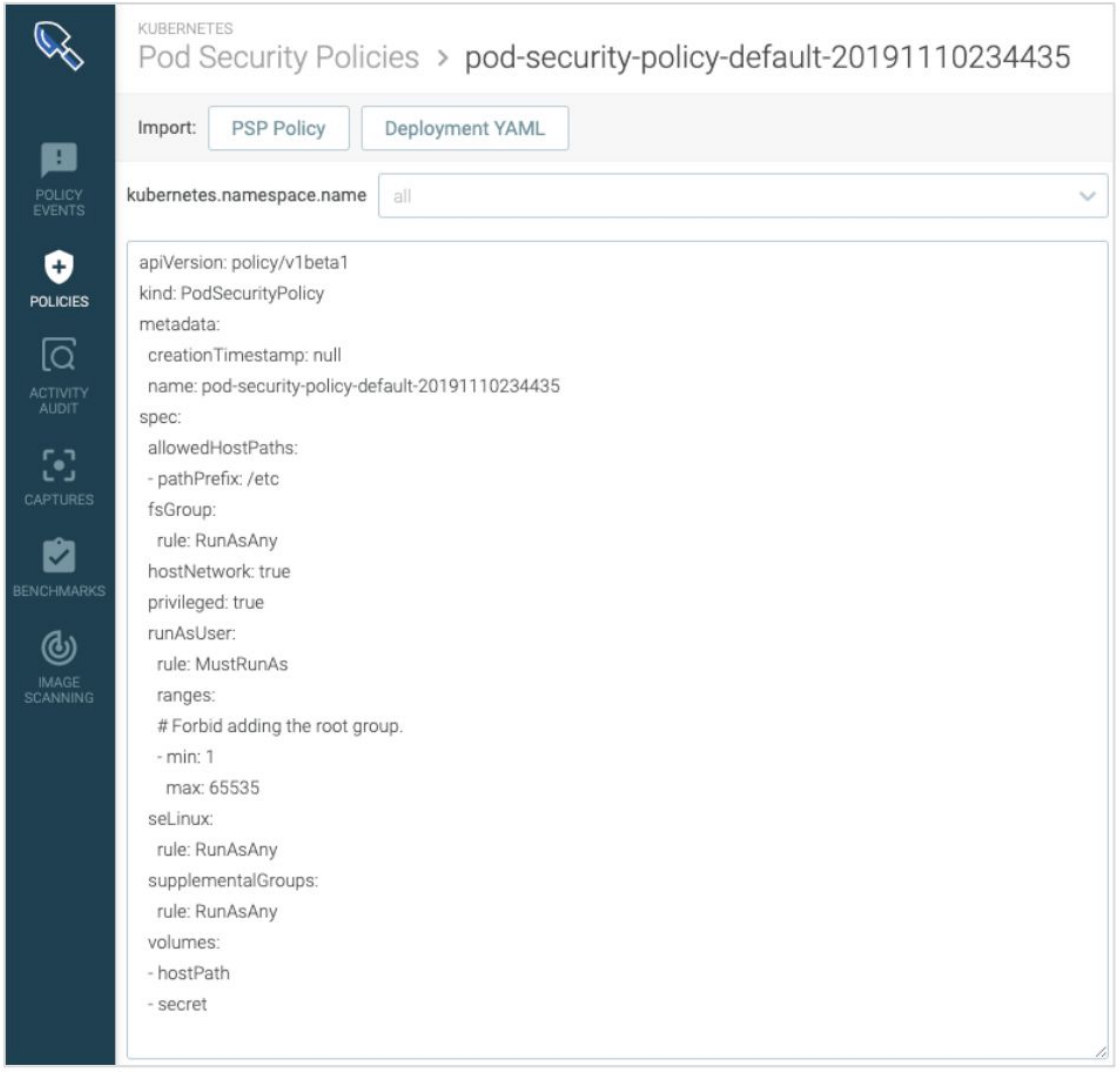
7.1.3 個々の担当者の職種と機能に基づいてアクセスを割り当てる

要件の説明

個々の従業員の職種と機能に基づいてアクセスを割り当てます。

Sysdigがどのように役立つか

Sysdigは、特定のネームスペースに固有のアプリケーションにおいて最小特権PSPを作成します。たとえば、permissive PSPをデフォルトとして作成し、アプリケーションのより機密性の高い部分である特定のネームスペースに対して特定のpermissive PSPを作成できます。



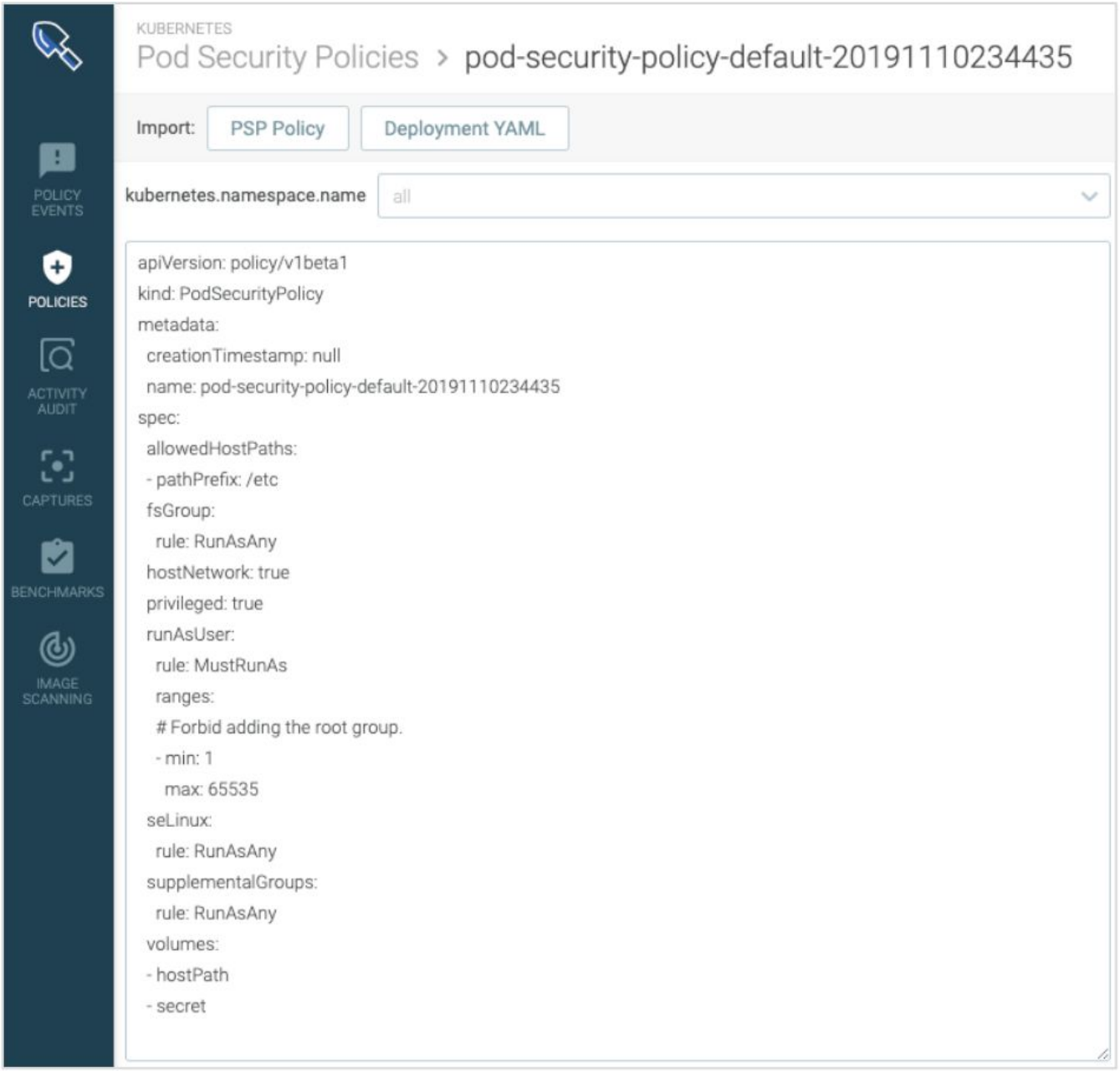
7.2.2 職種と職務に基づいて個人に特権を割り当てる

要件の説明

職種と職務に基づいた個人への特権の割り当て

Sysdigがどのように役立つか

Sysdigは、特定のネームスペースに固有のアプリケーションにおいて最小特権PSPを作成します。たとえば、permissive PSPをデフォルトとして作成し、アプリケーションのより機密性の高い部分である特定のネームスペースに対して特定のpermissive PSPを作成できます。


KUBERNETES
Pod Security Policies > pod-security-policy-default-20191110234435
Import:
PSP Policy
Deployment YAML
kubernetes.namespace.name
all
POLICY EVENTS
POLICIES
ACTIVITY AUDIT
CAPTURES
BENCHMARKS
IMAGE SCANNING
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
creationTimestamp: null
name: pod-security-policy-default-20191110234435
spec:
allowedHostPaths:
- pathPrefix: /etc
fsGroup:
rule: RunAsAny
hostNetwork: true
privileged: true
runAsUser:
rule: MustRunAs
ranges:
Forbid adding the root group.
- min: 1
max: 65535
seLinux:
rule: RunAsAny
supplementalGroups:
rule: RunAsAny
volumes:
- hostPath
- secret

7.2.3 デフォルトはすべて拒否設定

要件の説明

デフォルトは「すべて拒否」設定

Sysdigがどのように役立つか

Sysdigは、アプリケーションに対して最小限の特権のPSPを作成します。これは、非常に制限的であり、すべて拒否設定に従うように指定できます。 前述の例を参照してください。

要件10：

ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

ロギングメカニズムとユーザーアクティビティを追跡する機能は、データ侵害の影響を防止、検出、または最小化するために重要です。すべての環境にログが存在するため、何か問題が発生した場合に徹底的な追跡、アラート、分析が可能です。システムアクティビティログがないと、妥協の原因を特定することは不可能ではないにしても、非常に困難です。

10.1 各ユーザーへのアクセスをリンクする監査証跡を実装する

要件の説明

監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。

ガイドライン

ユーザーのアクセスをアクセスされるシステムコンポーネントにリンクするプロセスまたはシステムを持つことが重要です。このシステムは監査ログを生成し、疑わしいアクティビティを特定のユーザーにトレースバックする機能を提供します。

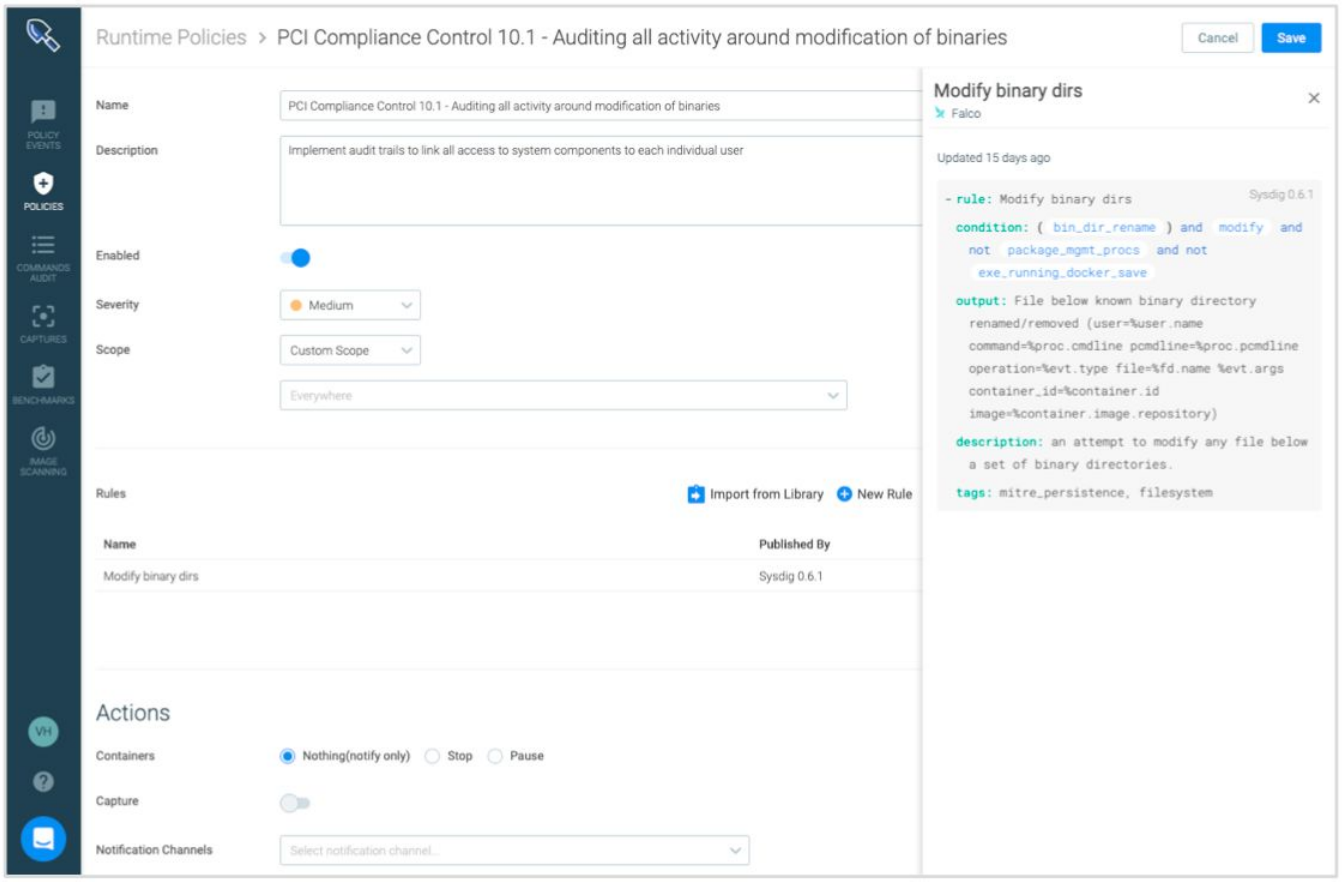
コンテナにおける課題

コンテナはLinuxカーネル内のcgroupとネーススペースから分離されているため、コンテナ内で実際に何が起こっているかを見るのは非常に困難です。また、ユーザーがコンテナ内で何かをしているときは、すべてがルートアクティビティのように見えるため、個々のユーザーをコンテナ内の特定のアクティビティに追跡することは非常に困難です。

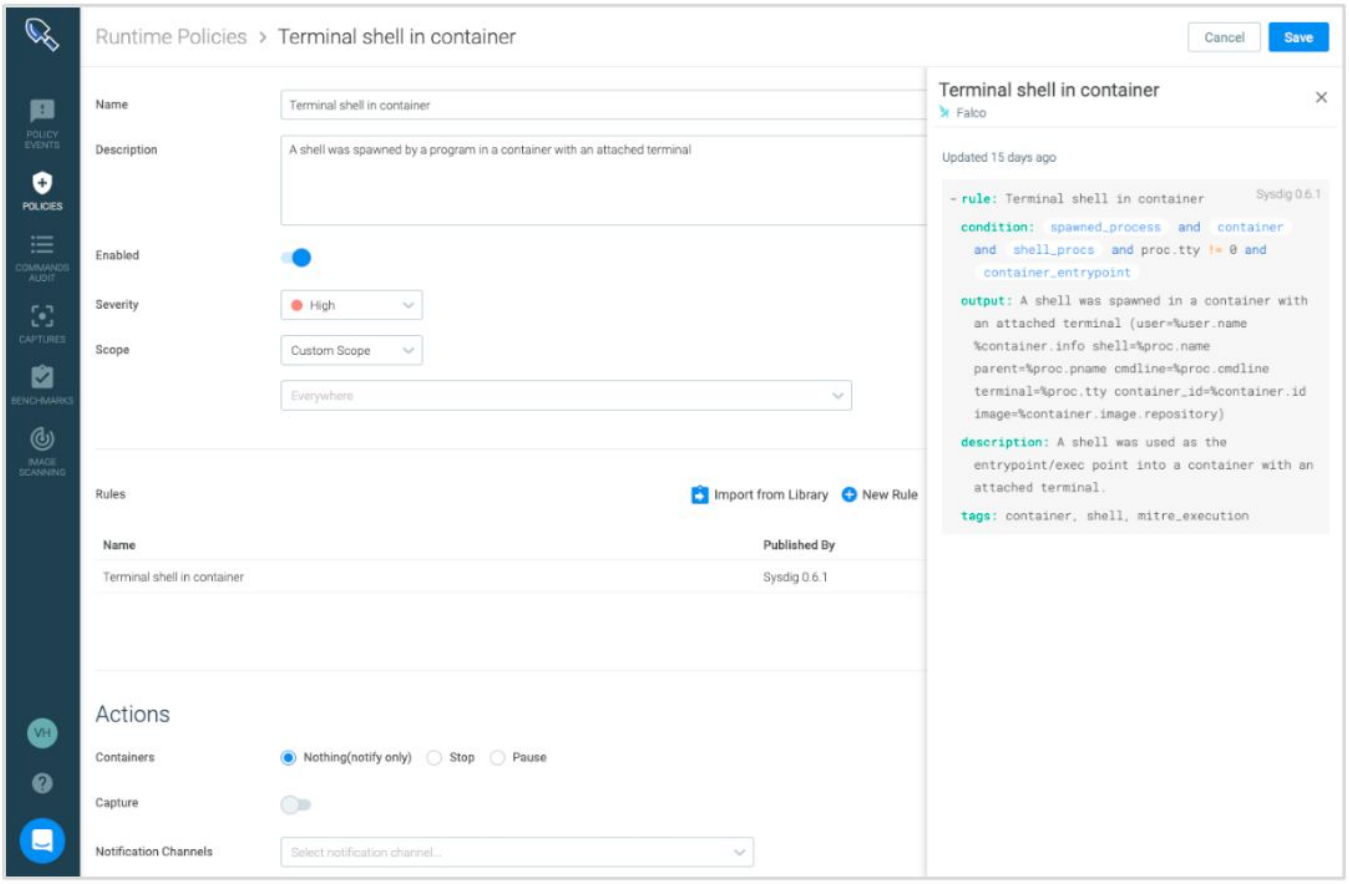
Sysdigがどのように役立つか

Sysdigはカーネルレベルで情報を取得している、セキュリティイベントの前、最中、および後のすべてのシステムアクティビティをキャプチャできます。Sysdig Secureは、コマンド引数、pid、ディレクトリなどを含むユーザーコマンドなどのシステムアクティビティを相関させ、Kubectlユーザーセッションと相関させます。

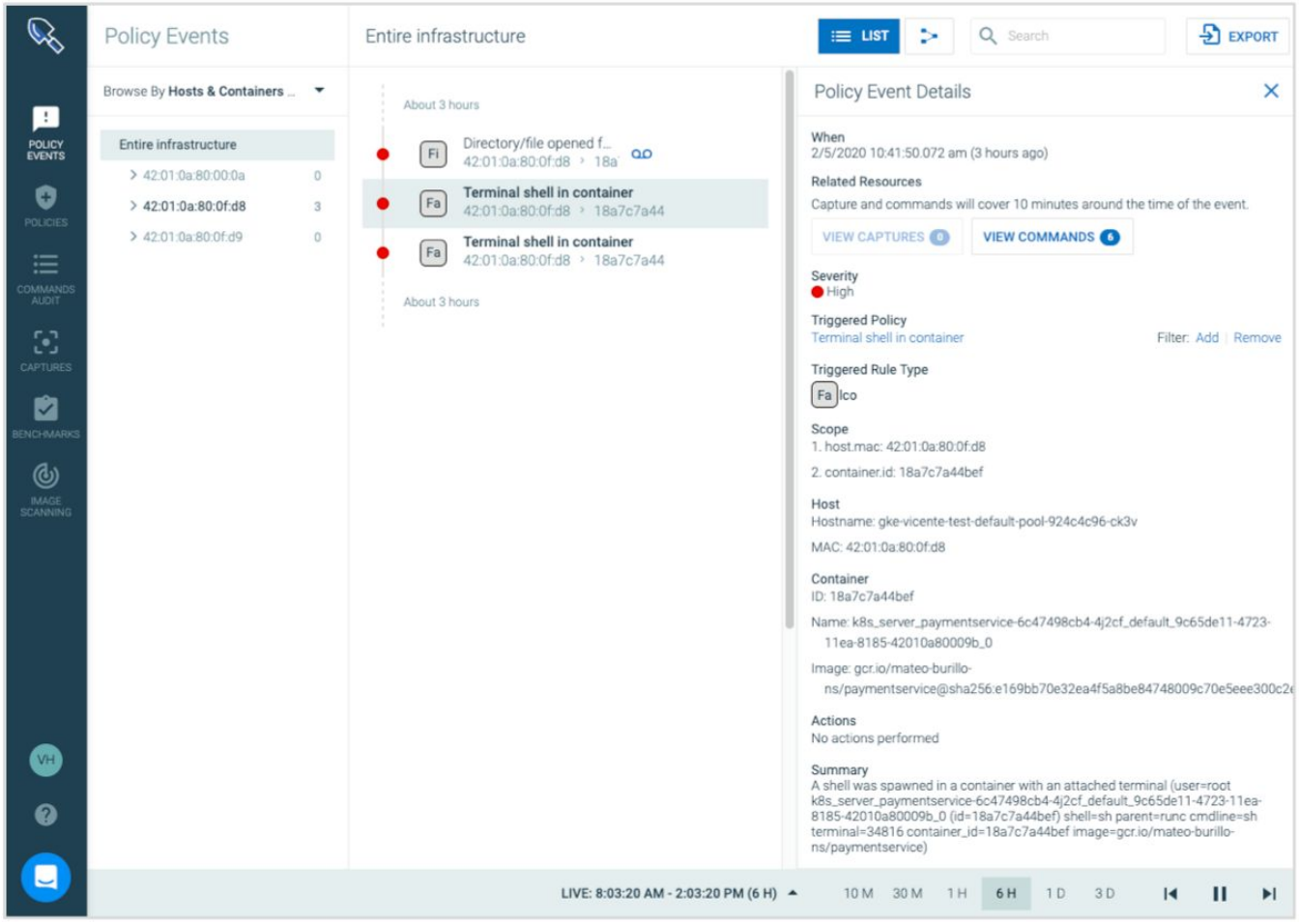
ユーザーがディレクトリ内のどこかにペイメントファイルがあるバイナリディレクトリを変更したかどうかを検出するルールの例

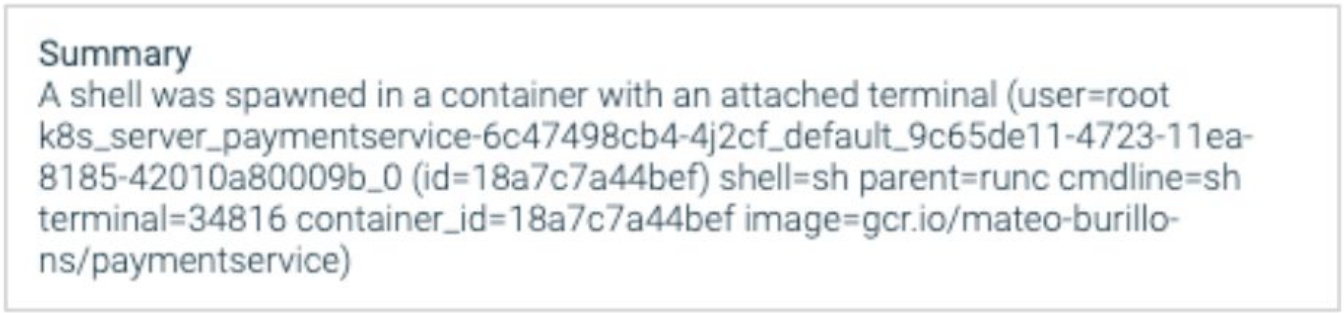


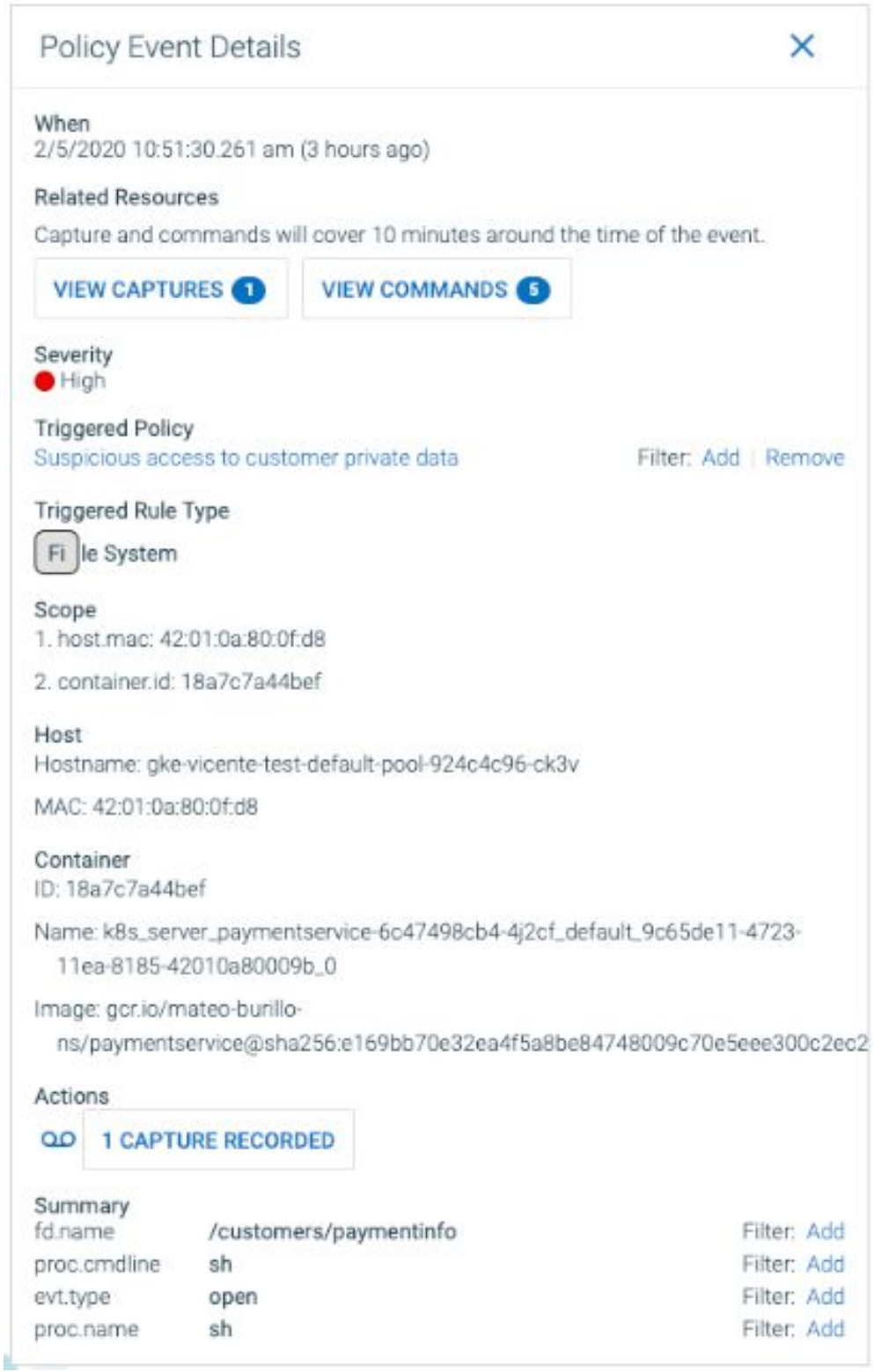
ユーザーが接続された端末がでシェルを生成したかどうかを検出するルールの例



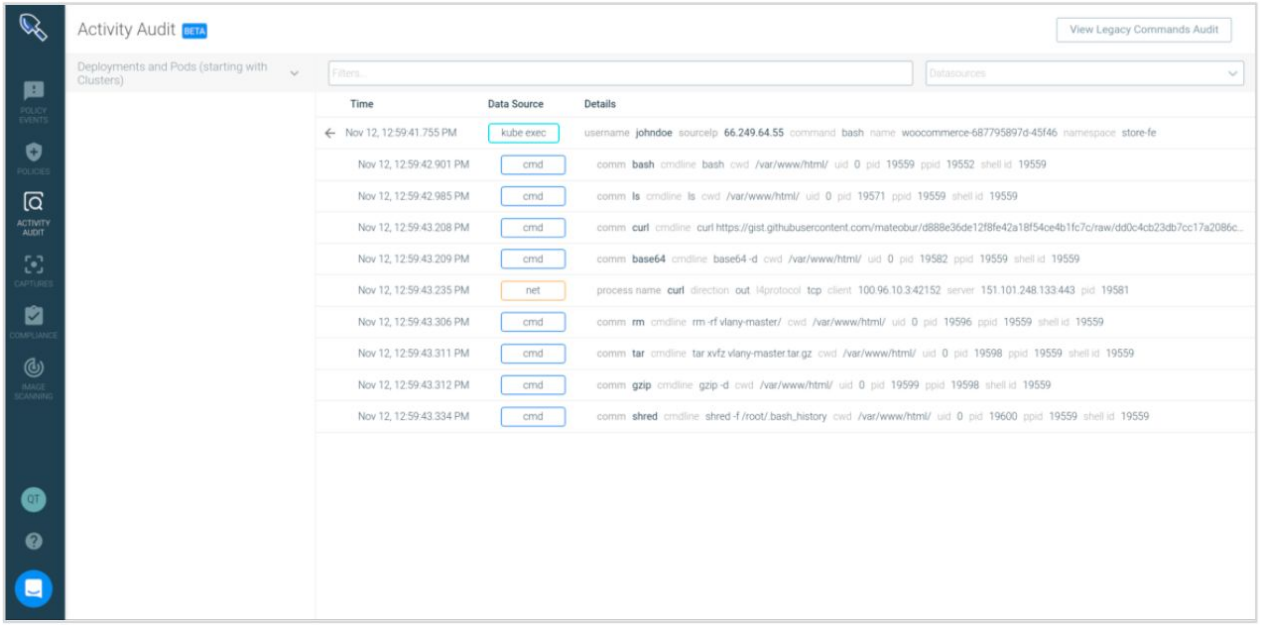
ユーザーがコンテナ内でシェルを生成し、機密のPANデータを読み取ることによってトリガーされるセキュリティイベント



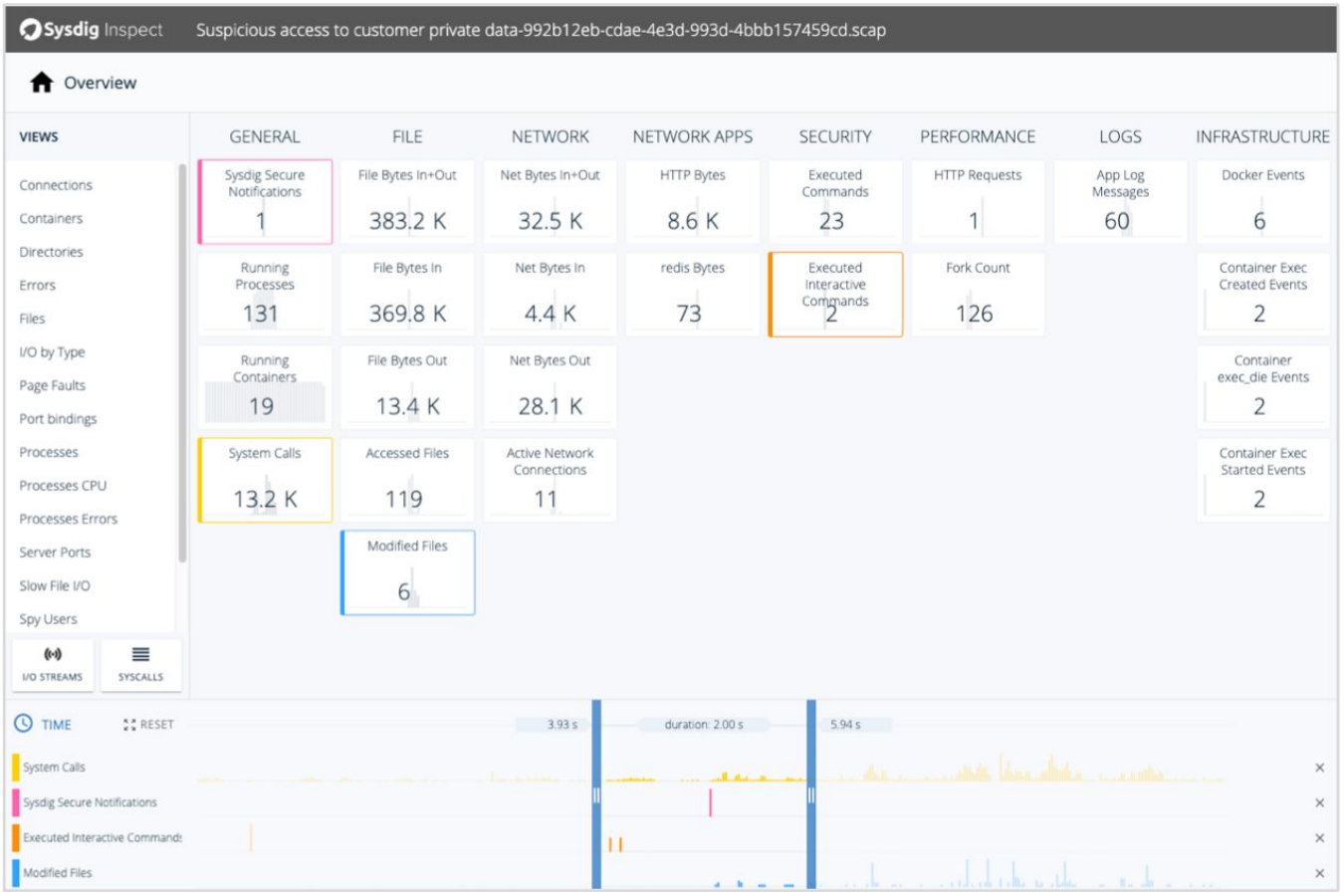



Policy Event Details
When
2/5/2020 10:51:30.261 am (3 hours ago)
Related Resources
Capture and commands will cover 10 minutes around the time of the event.
VIEW CAPTURES 1
VIEW COMMANDS 5
Severity
High
Triggered Policy
Suspicious access to customer private data
Filter: Add | Remove
Triggered Rule Type
File System
Scope
1. host.mac: 42:01:0a:80:0f:d8
2. container.id: 18a7c7a44bef
Host
Hostname: gke-vicente-test-default-pool-924c4c96-ck3v
MAC: 42:01:0a:80:0f:d8
Container
ID: 18a7c7a44bef
Name: k8s_server_paymentservice-6c47498cb4-4j2cf_default_9c65de11-4723-11ea-8185-42010a80009b_0
Image: gcr.io/mateo-burillo-ns/paymentservice@sha256:e169bb70e32ea4f5a8be84748009c70e5eee300c2ec2
Actions
1 CAPTURE RECORDED
Summary
fd.name /customers/paymentinfo Filter: Add
proc.cmdline sh Filter: Add
evt.type open Filter: Add
proc.name sh Filter: Add

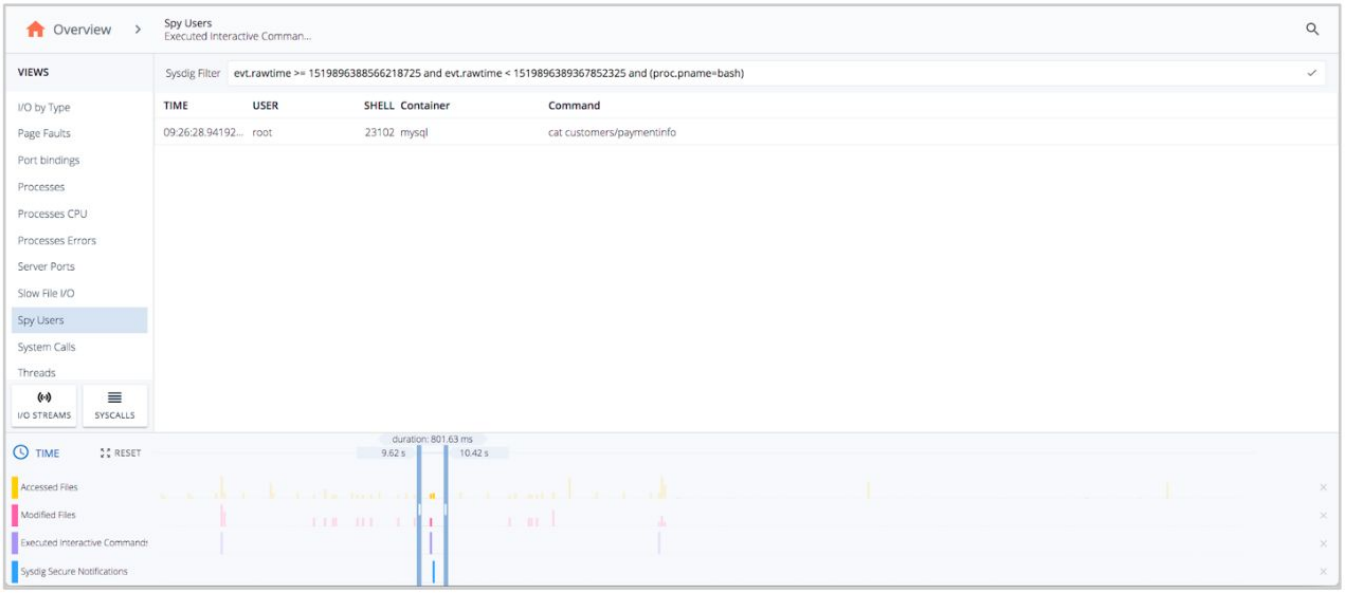
Activity Auditでは、Kubernetesユーザーがポッドを実行し、いくつかのコマンド（curl、bashなど）を実行して特定のファイルを読み取り、コンテナーを強制終了して証拠を消去したことがわかります。



Sysdig Inspectを使用すると、コンプライアンスチームとフォレンジックチームがシステム環境で行われていたすべての状況を把握できます。スライダーを使用して、特定のウィンドウをマイクロ秒の粒度で表示し、すべてのタイルの視覚化を更新できます。

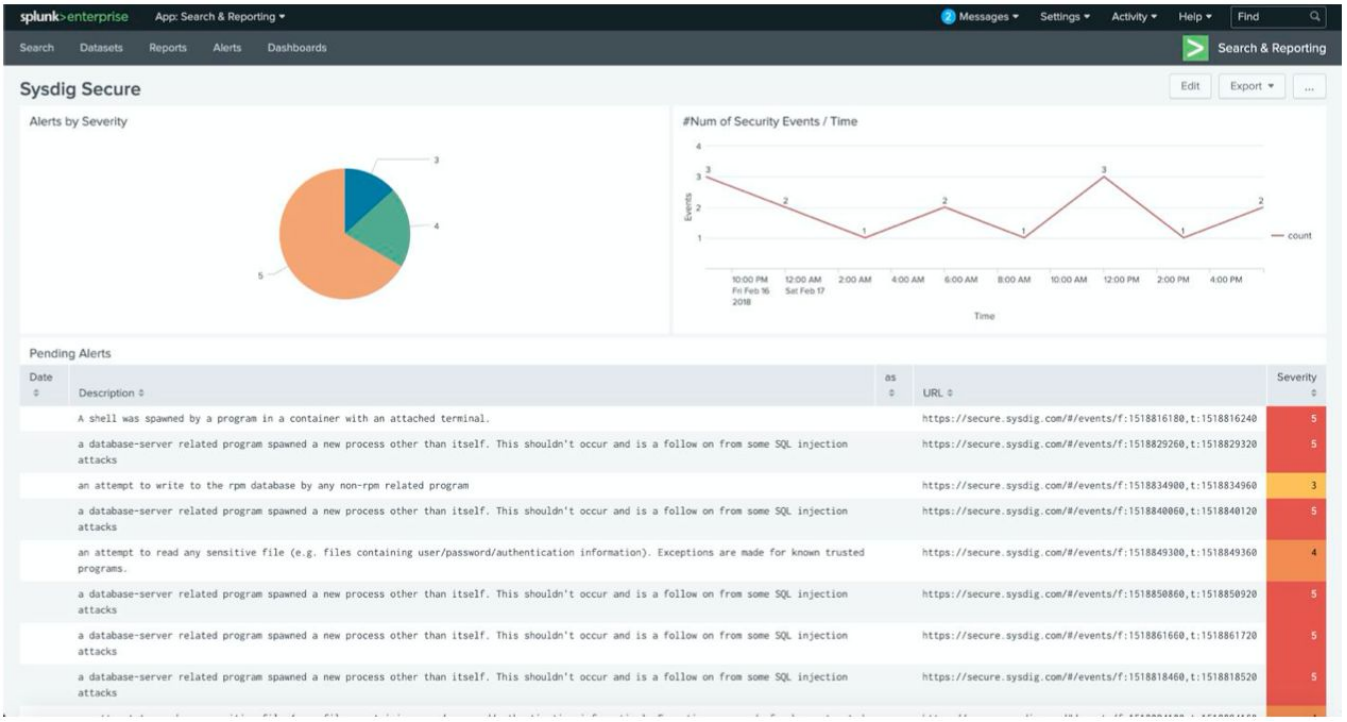


タイルをドリルダウンして、特定の実行済みコマンドを表示できます。この場合、ユーザーがcatコマンドを使用してPANで機密データを読み取る場所を確認できます。



I/O機能を使用して、読み取られたデータを明確に特定し、問題の範囲を迅速に判断する機能を備えています。

Sysdig Secureでは、監査関連イベントをSplunkなどのSIEMシステムに転送できます。



コンテナ内のターミナルシェルを検出するFalcoルール

```
- rule: Terminal shell in container

  desc: >
    A shell was used as the entrypoint/exec point into a container with an attached terminal

  condition: >

    spawned_process and container

    and shell_procs and proc.tty != 0

    and container_entrypoint

  output: >

    A shell was spawned in a container with an attached terminal
   (user=%user.name %container.info shell=%proc.name parent=%proc.pname
    cmdline=%proc.cmdline terminal=%proc.tty container_id=%container.id
    image=%container.image.repository)

  priority: NOTICE

  tags: [container, shell, mitre_execution, PCI, PCI_DSS_10.1]
```

10.2 自動監査証跡を実装してイベントを再構築する

要件の説明

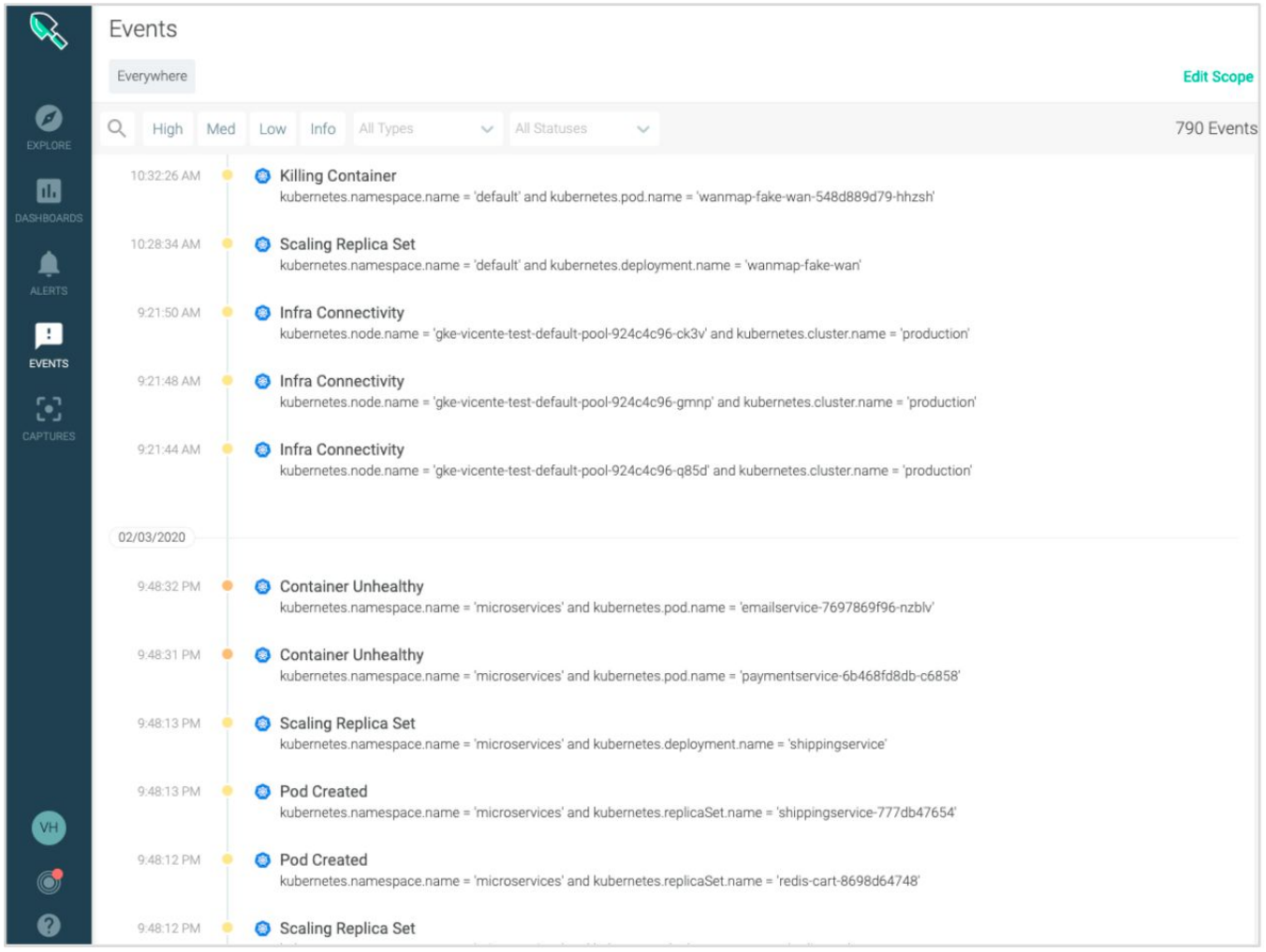
すべてのシステムコンポーネントに自動監査証跡を実装して、イベントを再構築します。

ガイドライン

疑わしいアクティビティの監査証跡を生成すると、システム管理者に警告が送られ、他の監視メカニズム（侵入検知システムなど）にデータが送信され、インシデント後のフォローアップの履歴証跡が提供されます。イベントのログを記録することにより、組織は潜在的に悪意のあるアクティビティを特定して追跡できます。

Sysdigがどのように役立つか

Sysdigは機能として提供している定義により、インフラストラクチャまたはクラウドリソースのメトリクスとセキュリティイベントを検出および監査するためのツールとして実現しています。したがって、その機能全体がこのセキュリティ要件を対象としています。また、既に示した多くの機能に加えて、すべてのクラスターで発生するKubernetesの監査イベントをSecureに追加する事ができます。このイベント監査では、イベントの優先度、時間枠、またはスコープ（クラスター、ネームスペースなど）でフィルタリングできます。



いくつかのFalcoルールは、監査したい特定のセキュリティイベントを追跡するのに役立ちます。

すべてのK8監査イベントを検出するFalcoルール

```
- rule: All K8s Audit Events

  desc: Match all K8s Audit Events

  condition: kall

  output: >

  K8s Audit Event received
  (user=%ka.user.name verb=%ka.verb uri=%ka.uri obj=%jevt.obj)

 priority: DEBUG

 source: k8s_audit

 tags: [k8s, PCI, PCI_DSS_10.2]
```

ワイルドカードを使用したClusterRoleの作成を検出するFalcoルール

```
- rule: ClusterRole With Wildcard Created

  desc: Detect any attempt to create a Role/ClusterRole with wildcard resources or verbs

  condition: >

    kevt and (role or clusterrole) and kcreate and
    (ka.req.role.rules.resources intersects ("*") or
     ka.req.role.rules.verbs intersects ("*"))

  output: >
    Created Role/ClusterRole with wildcard
    (user=%ka.user.name role=%ka.target.name rules=%ka.req.role.rules)

  priority: WARNING

  source: k8s_audit

  tags: [k8s, PCI, PCI_DSS_10.2]
```

書き込み権限を持つClusterRoleの作成を検出するFalcoルール

```
- rule: ClusterRole With Write Privileges Created

  desc: >
    Detect any attempt to create a Role/ClusterRole that can perform write-related actions

  condition: kevt and (role or clusterrole) and kcreate and writable_verbs

  output: >

    Created Role/ClusterRole with write privileges
    (user=%ka.user.name role=%ka.target.name rules=%ka.req.role.rules)

   priority: NOTICE

   source: k8s_audit

   tags: [k8s, PCI, PCI_DSS_10.2]
```

Pod ExecでClusterRoleの作成を検出するFalcoルール

```
- rule: ClusterRole With Pod Exec Created

  desc: Detect any attempt to create a Role/ClusterRole that can exec to pods

  condition: >

    kevt and (role or clusterrole) and
    kcreate and
    ka.req.role.rules.resources intersects ("pods/exec")

  output: >
    Created Role/ClusterRole with pod exec privileges

    (user=%ka.user.name role=%ka.target.name rules=%ka.req.role.rules)

  priority: WARNING

  source: k8s_audit

  tags: [k8s, PCI, PCI_10.2]
```

10.2.1 すべての個人ユーザーにおけるカード会員データへのアクセス

要件の説明

すべての個々のユーザーがカード会員データにアクセスします。

ガイドライン

悪意のある個人は、CDEのシステムにアクセスできるユーザーアカウントの情報を取得したり、カード会員データにアクセスするために新しい無許可のアカウントを作成したりする可能性があります。 カード会員データへのすべての個人アクセスの記録により、どのアカウントが侵害または悪用された可能性があるかを特定できます。

コンテナにおける課題

ファイルアクセスをユーザーに戻すことは、特にコンテナ内でアクションが実行される場合に困難になることがよくあります。 また、コンテナのエフェメラルな性質により、コンテナを起動し、データの抽出アクティビティを完了してから、ほんの数秒で終わらせることができます。

Sysdigがどのように役立つか

10.1の例を参照してください

10.2.2 ルートまたは管理者権限を持つ個人によって行われたすべてのアクション

要件の説明

ルートまたは管理者権限を持つ個人が実行するすべてのアクション

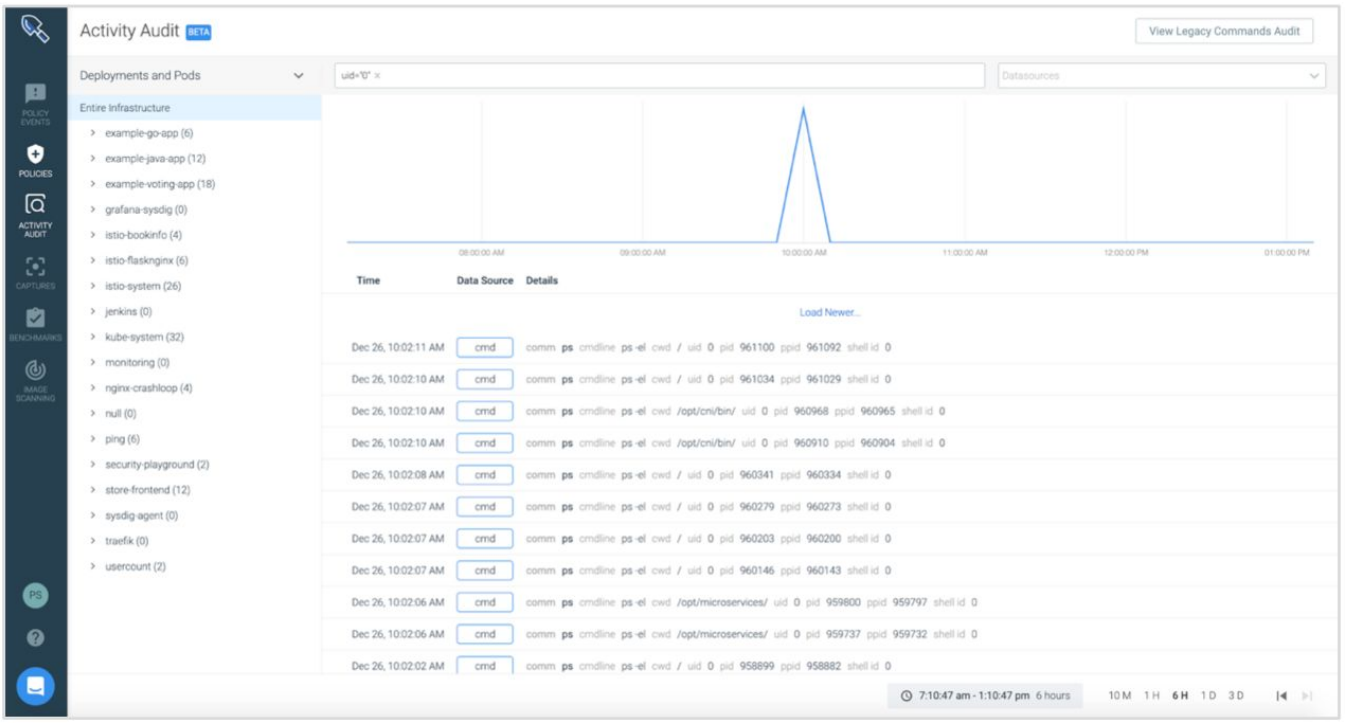
ガイドライン

「管理者」または「ルート」アカウントなど、権限が増加したアカウントは、システムのセキュリティまたは運用機能に大きな影響を与える可能性があります。実行されたアクティビティのログがないと、組織は管理上のミスや特権の誤用に起因する問題を特定のアクションや個人にまでさかのぼることができません。

Sysdigがどのように役立つか

デフォルトでは、Sysdigは、ホスト上およびコンテナ内でユーザーが実行したすべてのアクションをキャプチャします。これらのアクションは、ホスト、コンテナ、またはオーケストレーションのメタデータに基づいて表示することもでき、コマンドがインフラストラクチャ全体でラテラルムーブメントをトリガーする方法を表示できます。

ユーザーコマンドをフィルター処理して、実行されたすべてのルート（uid = 0）コマンドを分離



10.2.5 識別および認証メカニズムの使用と変更

要件の説明

新しいアカウントの作成や特権の昇格などの識別および認証メカニズムの使用と変更、およびルートまたは管理者特権を持つアカウントに対するすべての変更、追加、削除

ガイドライン

インシデント発生時に誰がログオンしていたかを知らなければ、使用された可能性のあるアカウントを特定することは不可能です。さらに、悪意のあるユーザーは、それらをバイパスしたり、有効なアカウントになりすますことを目的として、認証コントロールを操作しようとする場合があります。

Sysdigがどのように役立つか

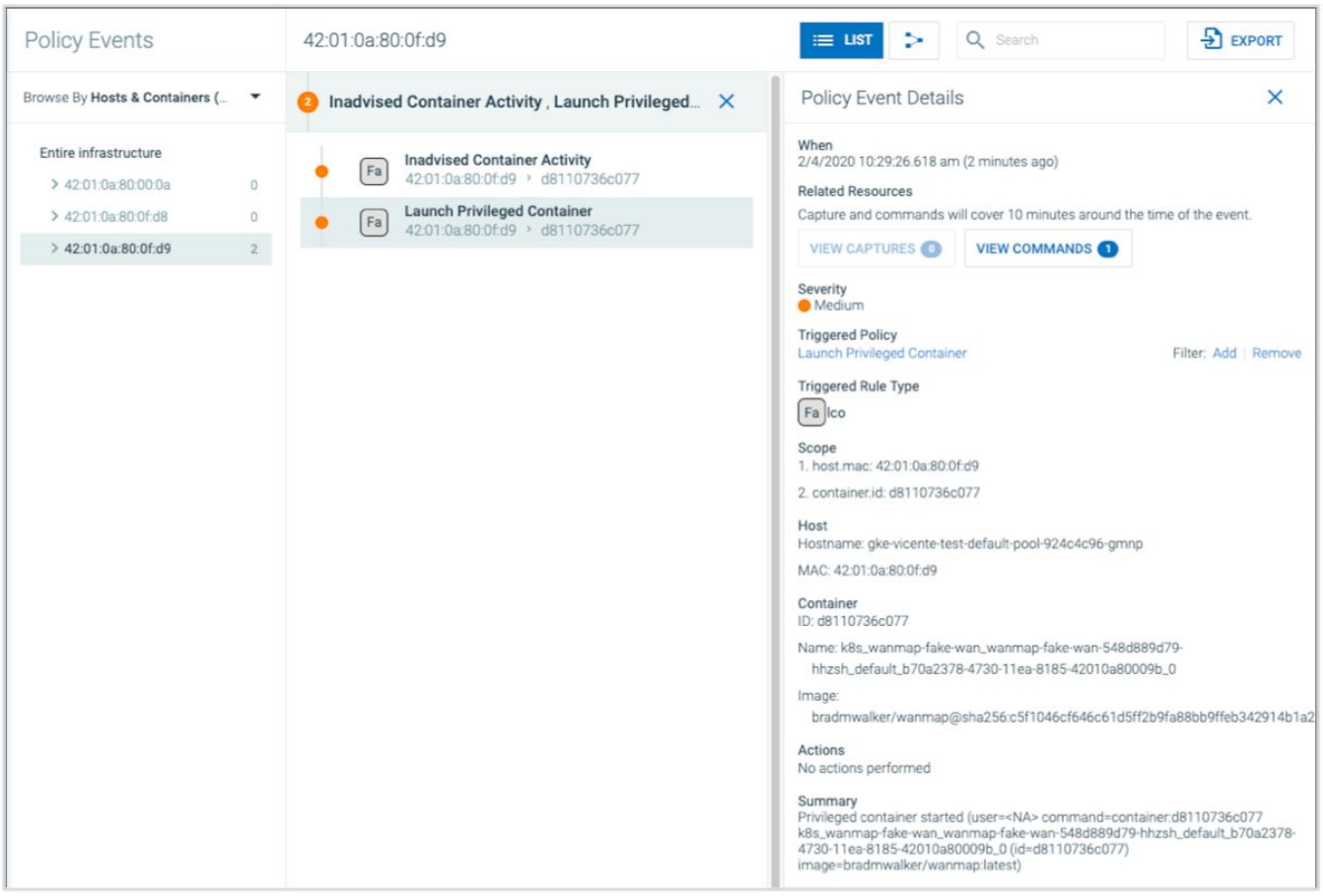
特権コンテナが起動されたかどうかを追跡するデフォルトポリシーがあり、以下のようにカスタムポリシーを簡単に作成して特権昇格の動作を探すことができます。

特権コンテナの起動を検出するFalcoルール

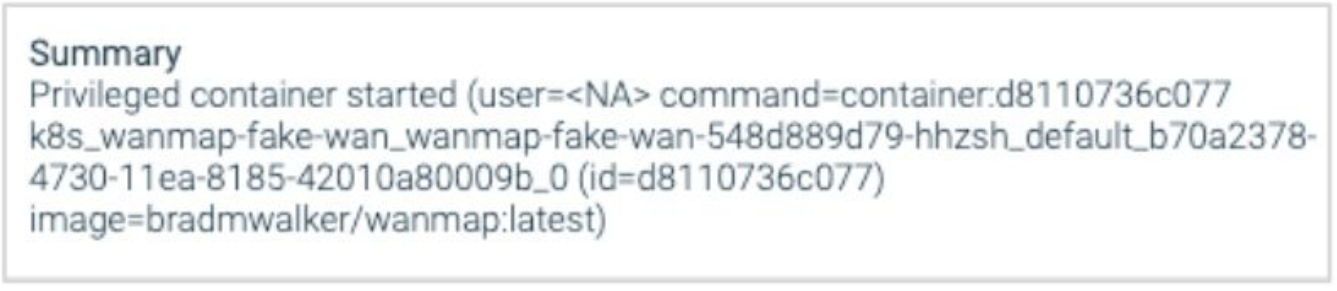
```
- rule: Launch Privileged Container

  desc: >
    Detect the initial process started in a privileged container.
    Exceptions are made for known trusted images.

  condition: >

    container_started and container

    and container.privileged=true

    and not falco_privileged_containers

    and not user_privileged_containers

  output: >
    Privileged container started
    (user=%user.name command=%proc.cmdline %container.info

    image=%container.image.repository:%container.image.tag)
```

```
  priority: INFO

  tags: [container, cis, mitre_privilege_escalation, mitre_lateral_movement, \
    PCI, PCI_DSS_10.2.5]
```

コンテナーが特権モードで実行されているかどうかを調べるFalcoルール。たとえば、docker exec を実行しているユーザーに特権が渡される場合



ポッドで開始された特権コンテナーを検出するポリシーイベント通知



10.2.6 初期化、停止、一時停止のログ

要件の説明

初期化、停止、または一時停止の監査ログ

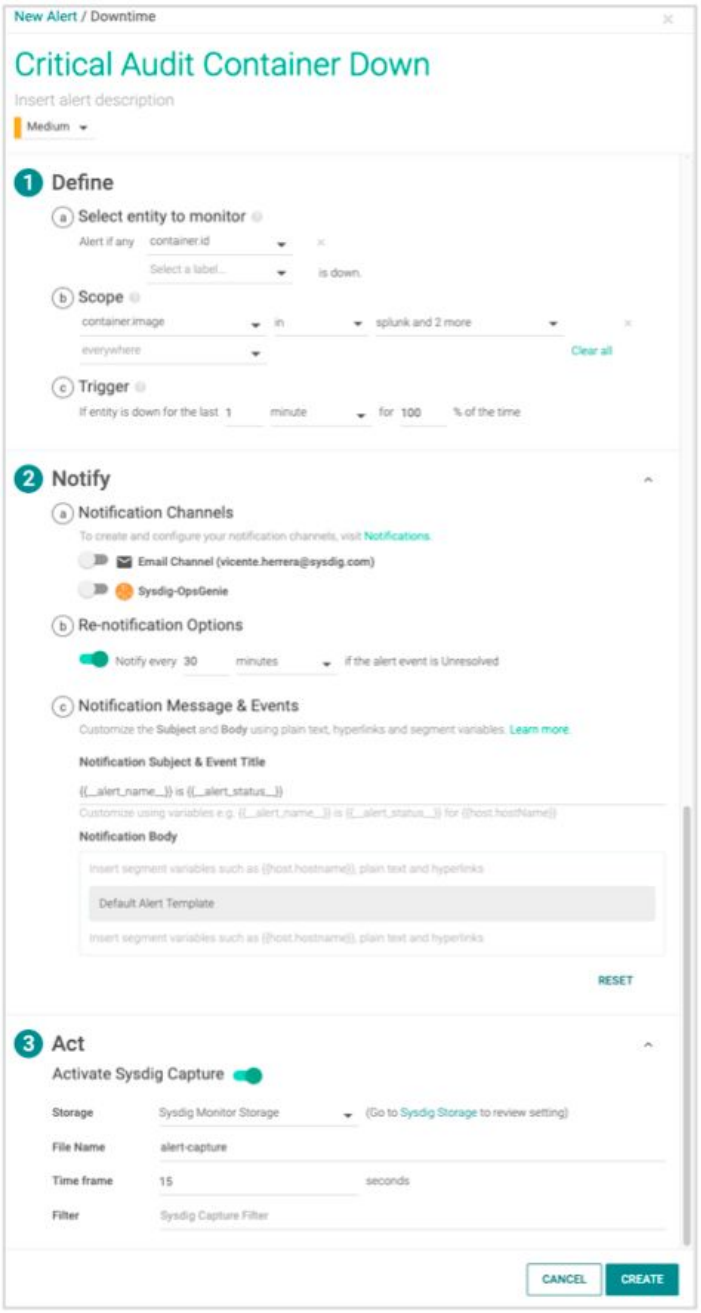
ガイドライン

不正なアクティビティを実行する前に監査ログをオフにする（または一時停止する）ことは、検出を避けたい悪意のあるユーザーにとって一般的な方法です。監査ログの初期化は、ユーザーがアクションを非表示にするためにログ機能が無効にされたことを示している場合があります。

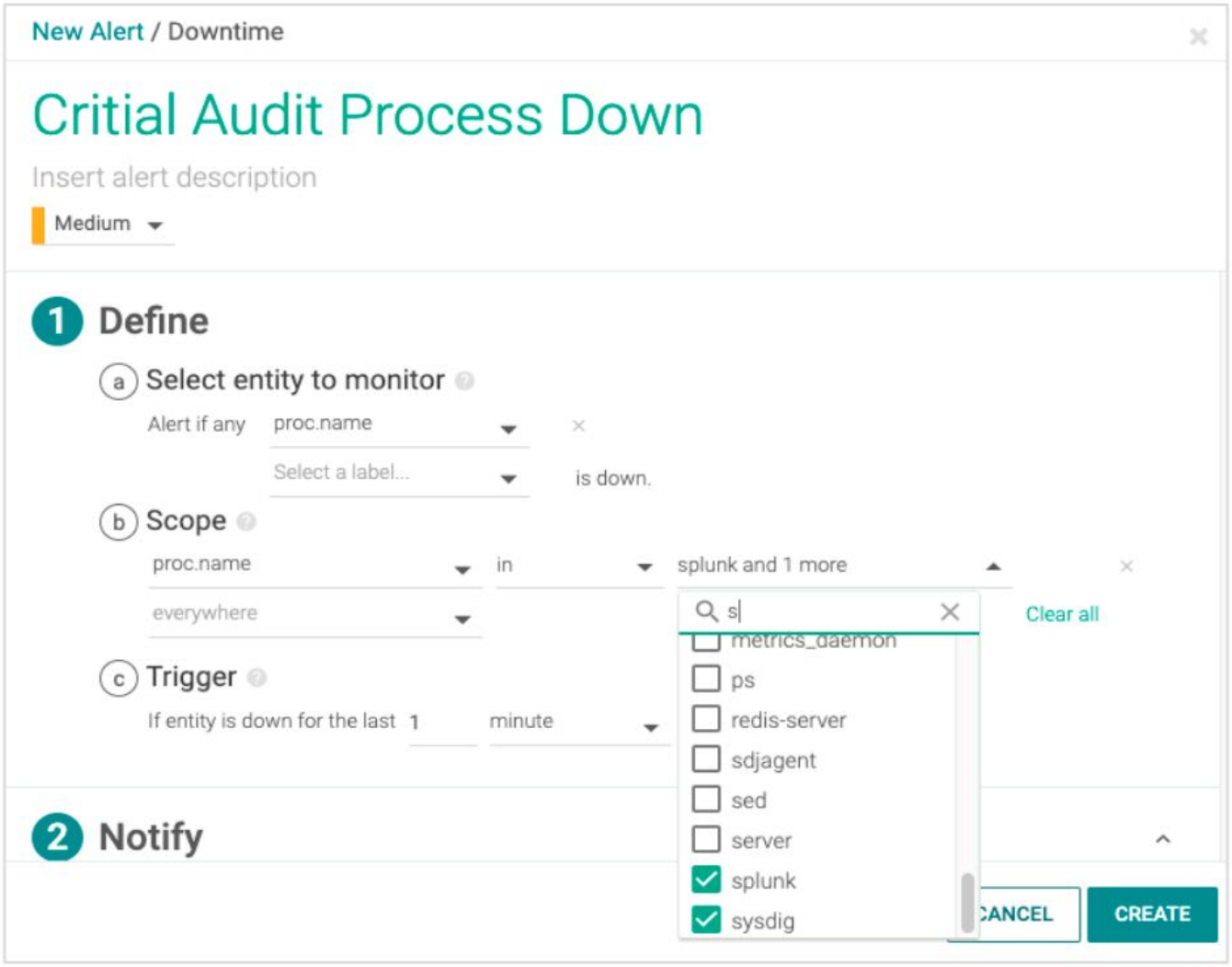
Sysdigがどのように役立つか

Sysdigは、デフォルトで、監視するすべてのエンティティの稼働時間メトリクスを追跡します。これらは、コンテナ、ホスト、kubernetesサービス、クラウドリージョンなどです。これらのサービスのいずれかがダウンしたり、削除されたりした場合は警告できます。

特定のコンテナがダウンの場合、splunk、Sysdigなどに警告します。このリストは自動的に入力され、簡単に変更できます。



プロセスに対しても同じことができます。 多くの場合、監査はホストで行われ、コンテナ情報も使用します。



10.2.7 作成/削除システムレベルのオブジェクト

要件の説明

システムレベルのオブジェクトの作成と削除

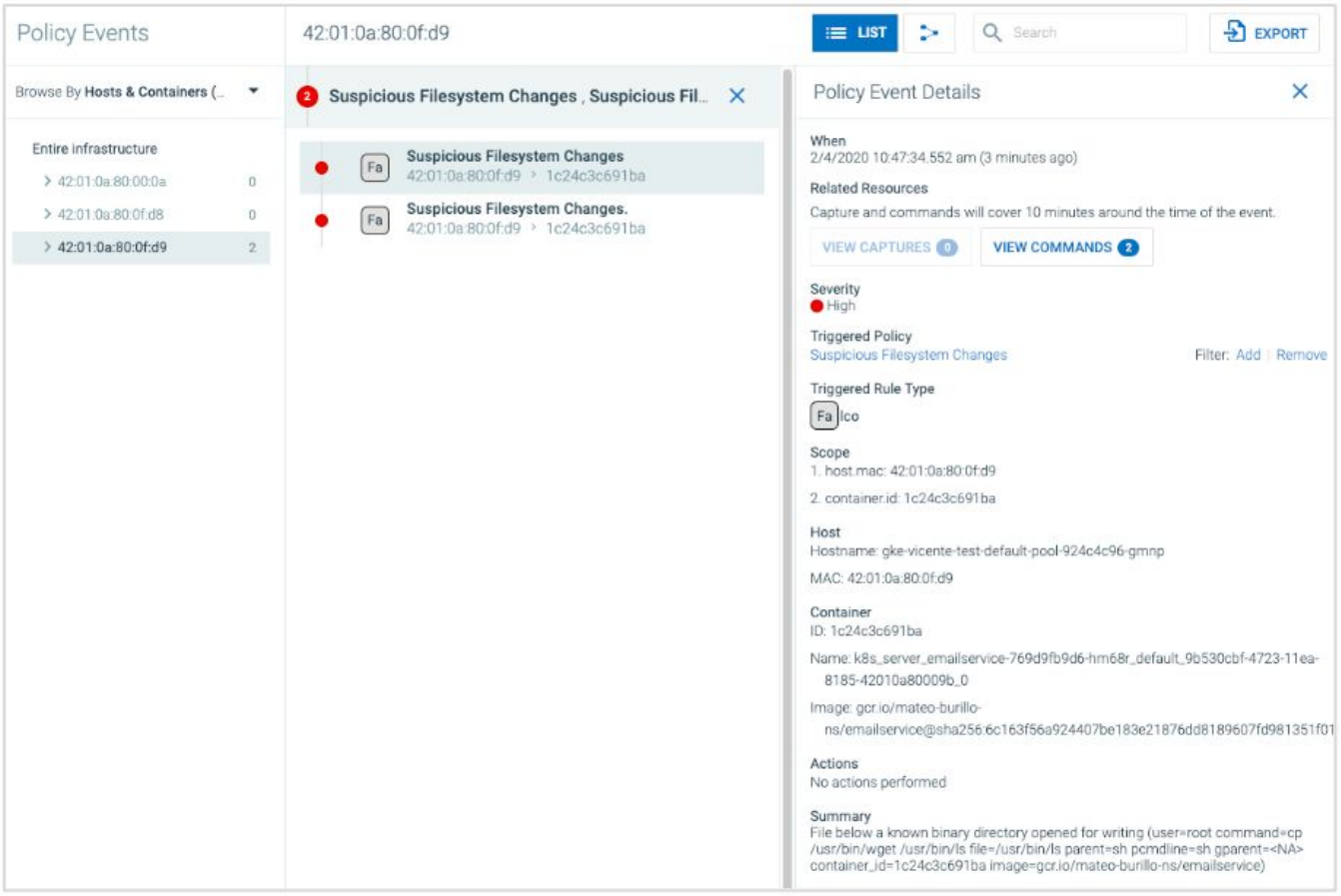
ガイドライン

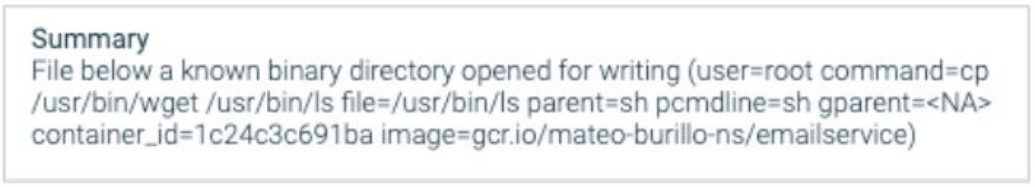
マルウェアなどの悪意のあるソフトウェアは、多くの場合、ターゲットシステム上で特定の機能または操作を制御するために、システムレベルのオブジェクトを作成または置換します。データベーステーブルやストアドプロシージャなどのシステムレベルのオブジェクトが作成または削除されたときにログを記録することにより、そのような変更が許可されたかどうかを簡単に判断できます。

Sysdigがどのように役立つか

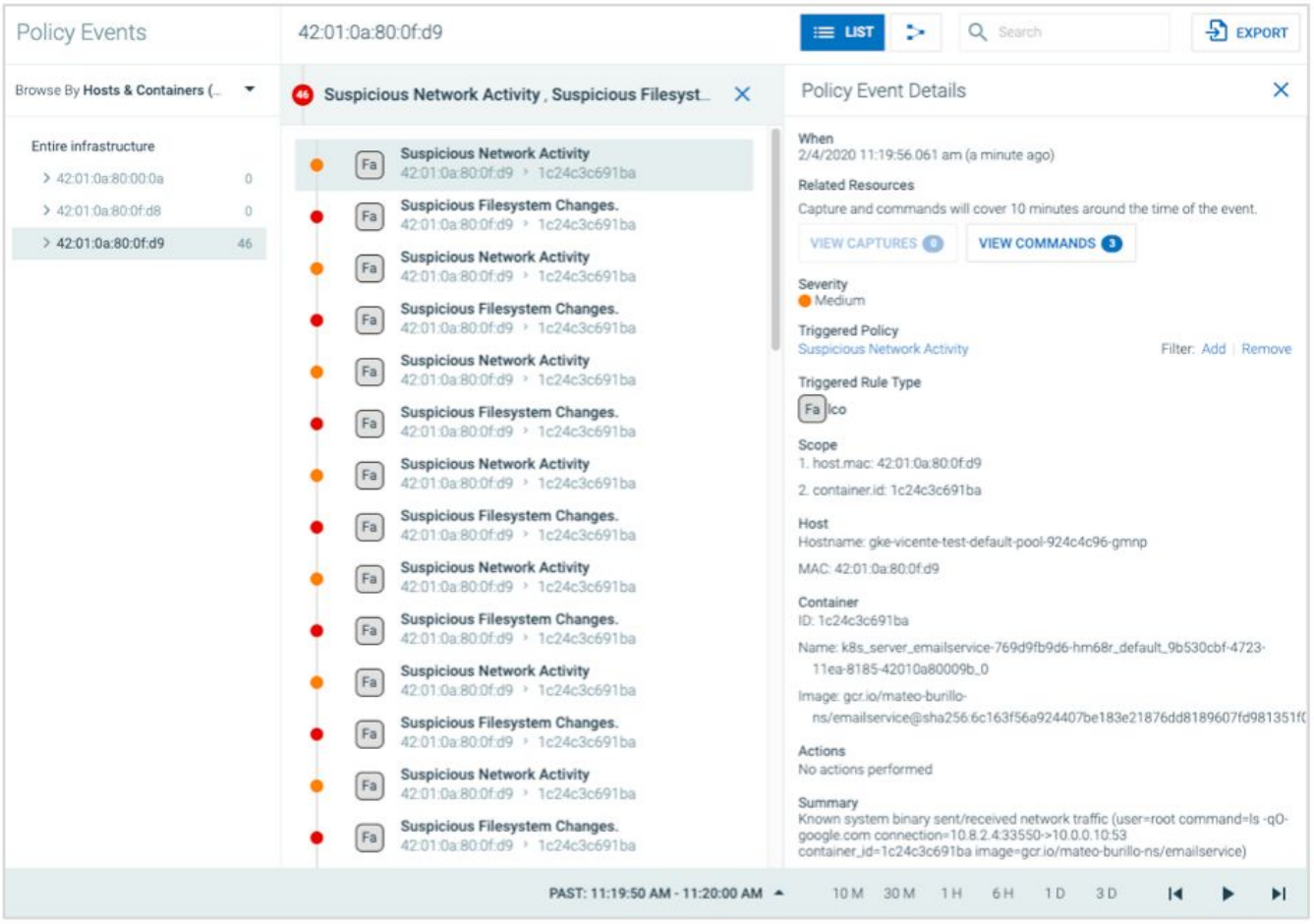
Sysdigには、異なるシステムバイナリと組み込みコマンドが置き換えられるかどうかを監視するデフォルトのポリシーがあります。

イベントの詳細から、ユーザーが「ls」機能を「wget」に置き換えたことがわかります。 つまり、ユーザーは「ls」を使用してインターネットからデータをプルできるようになりました。





この2番目のデフォルトポリシーは、既知のシステムバイナリ（ls）がネットワークトラフィックを送信したことを検出します。



Summary
Known system binary sent/received network traffic (user=root command=ls -qO- google.com connection=10.8.2.4:33550->10.0.0.10:53 container_id=1c24c3c691ba image=gcr.io/mateo-burillo-ns/emailservice)

バイナリディレクトリへの変更を検出するFalcoルール

```
- rule: Modify binary dirs

  desc: an attempt to modify any file below a set of binary directories.

  condition: >
    (bin_dir_rename) and modify and not package_mgmt_procs and not exe_running_docker_save

  output: >

    File below known binary directory renamed/removed
    (user=%user.name command=%proc.cmdline pcmdline=%proc.pcmdline operation=%evt.type

    file=%fd.name %evt.args container_id=%container.id image=%container.image.repository)

  priority: ERROR

  tags: [filesystem, mitre_persistence, PCI, PCI_DSS_10.2.7]
```

バイナリディレクトリ内のディレクトリの作成を検出するFalcoルール

```
- rule: Mkdir binary dirs

  desc: an attempt to create a directory below a set of binary directories.

  condition: mkdir and bin_dir_mkdir and not package_mgmt_procs

  output: >

    Directory below known binary directory created
    (user=%user.name command=%proc.cmdline directory=%evt.arg.path
    container_id=%container.id image=%container.image.repository)

  priority: ERROR

  tags: [filesystem, mitre_persistence, PCI, PCI_DSS_10.2.7]
```

10.3 イベントの監査証跡を記録する

要件の説明

各イベントのすべてのシステムコンポーネントについて、少なくとも以下の監査証跡エントリを記録します。

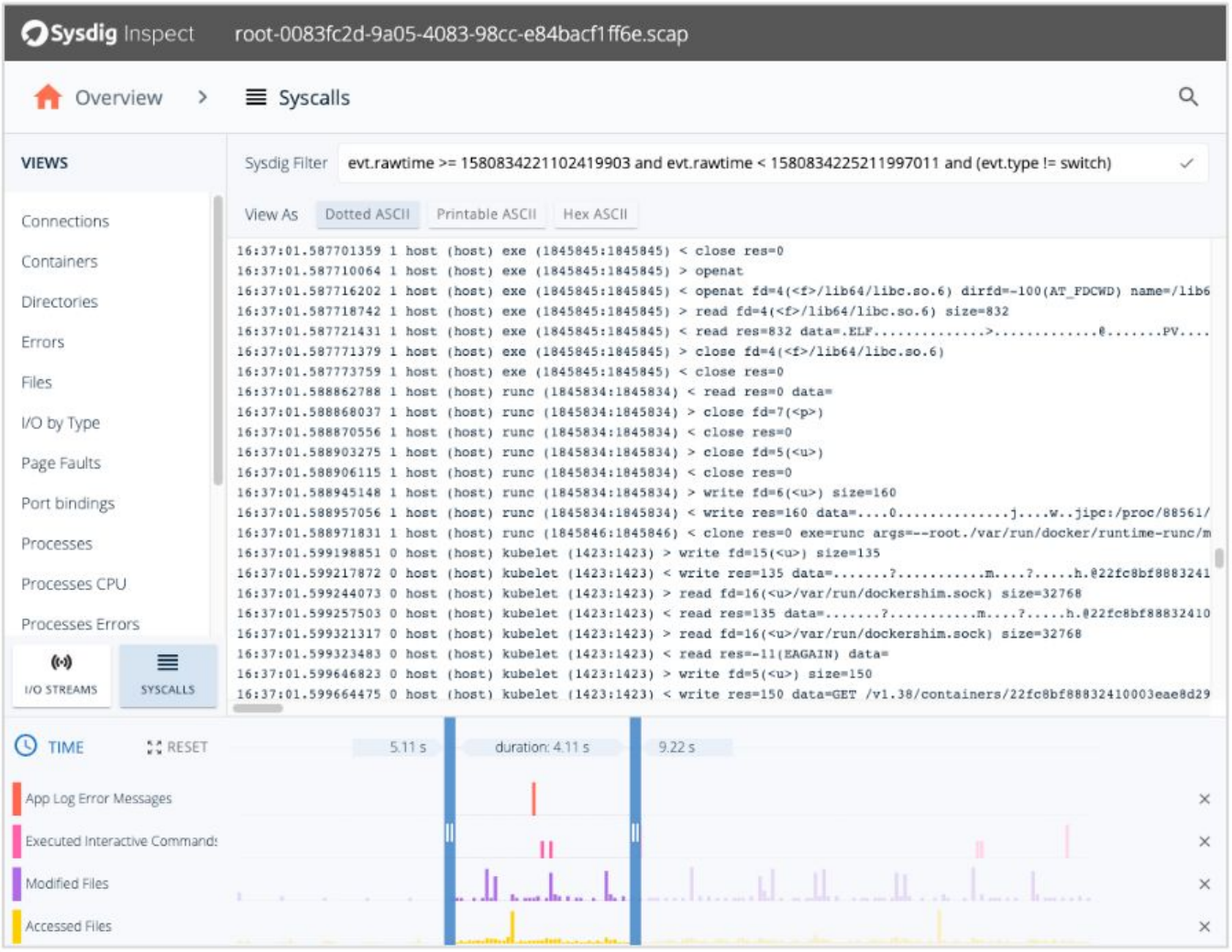
- 10.3.1 ユーザー識別
- 10.3.2 イベントのタイプ
- 10.3.3 日付と時刻
- 10.3.4 成功または失敗の表示
- 10.3.5 イベントの発生

ガイドライン

10.2で監査可能なイベントのこれらの詳細を記録することにより、潜在的な妥協点を迅速に特定でき、誰が、何を、どこで、いつ、どのように知るのに十分な詳細を備えています。

Sysdigがどのように役立つか

すべてのユーザーイベントには、発生したすべてのシステムコールレベルまでの完全なタイムスタンプがあります。



10.5.5 ログは変更できない事

要件の説明

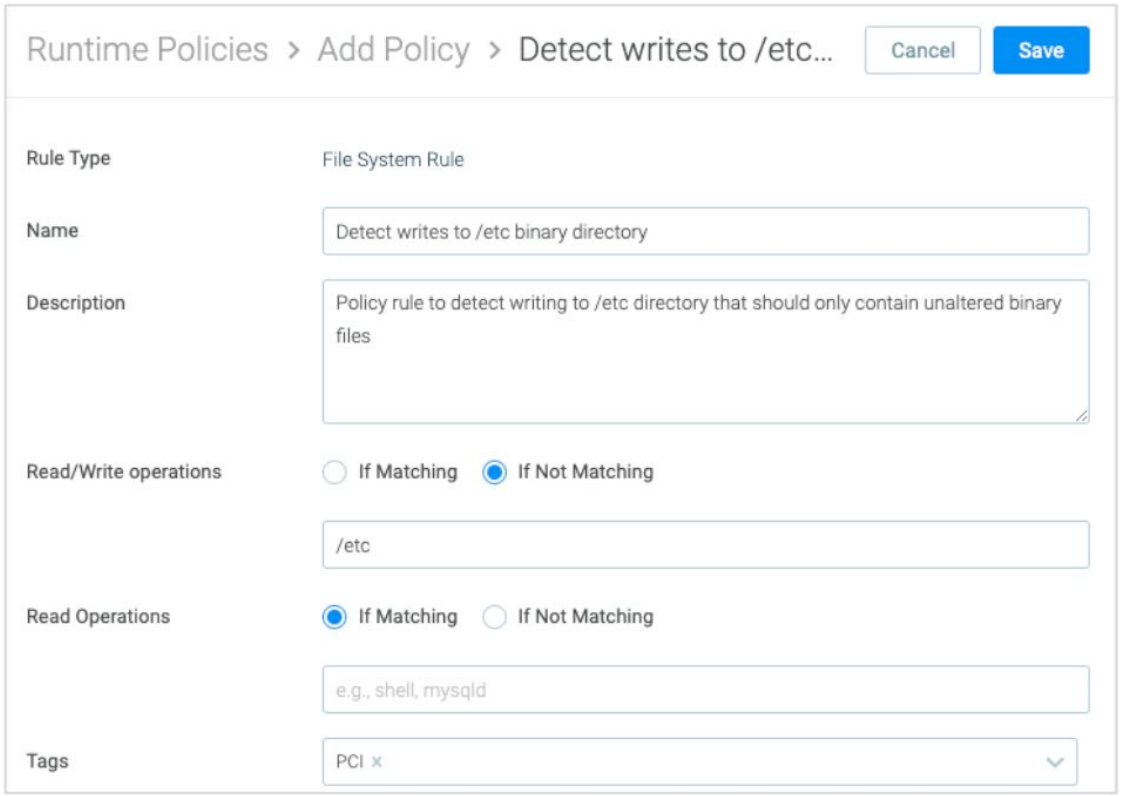
ログでファイル整合性監視または変更検出ソフトウェアを使用して、アラートを生成せずに既存のログデータを変更できないことを確認します（ただし、新しいデータを追加してもアラートは発生しません）

ガイドライン

ファイルの完全性の監視または変更検出システムは、重要なファイルへの変更をチェックし、そのような変更が記録されたときに通知します。ファイルの整合性を監視する目的で、エンティティは通常、定期的に変更されないファイルを監視しますが、変更された場合は侵害の可能性を示します。

Sysdigがどのように役立つか

すべてのファイルアクティビティを簡単に監視でき、高度なFalcoルールを使用してすべてのI/Oアクティビティを検査することもできます。



ログの変更を検出するFalcoルール

```
- list: log_directories

  items: [/var/log, /dev/log]

- list: log_files

  items: [syslog, auth.log, secure, kern.log, cron, user.log, dpkg.log, last.log, yum.log,
access_log, mysql.log, mysqld.log]

- macro: access_log_files

  condition: (fd.directory in (log_directories) or fd.filename in (log_files))

# a placeholder for whitelist log files that could be cleared. Recommend the macro as
(fd.name startswith "/var/log/app1*")

- macro: allowed_clear_log_files

  condition: (never_true)

- macro: trusted_logging_images

  condition: (container.image.repository endswith "splunk/fluentd-hec" or

              container.image.repository endswith "fluent/fluentd-kubernetes-daemonset")

- rule: Clear Log Activities

  desc: Detect clearing of critical log files

  condition: >

    open_write and

    access_log_files and

    evt.arg.flags contains "O_TRUNC" and

    not trusted_logging_images and
```

```
  not allowed_clear_log_files

output: >

  Log files were tampered
  (user=%user.name command=%proc.cmdline file=%fd.name container_id=%container.id
  image=%container.image.repository)

priority: WARNING

tags: [file, mitre_defense_evasion, PCI, PCI_DSS_10.5.5]
```

10.6.1 すべてのセキュリティイベントの日次レビュー

要件の説明

少なくとも日次で以下を確認してください-すべてのセキュリティイベント。

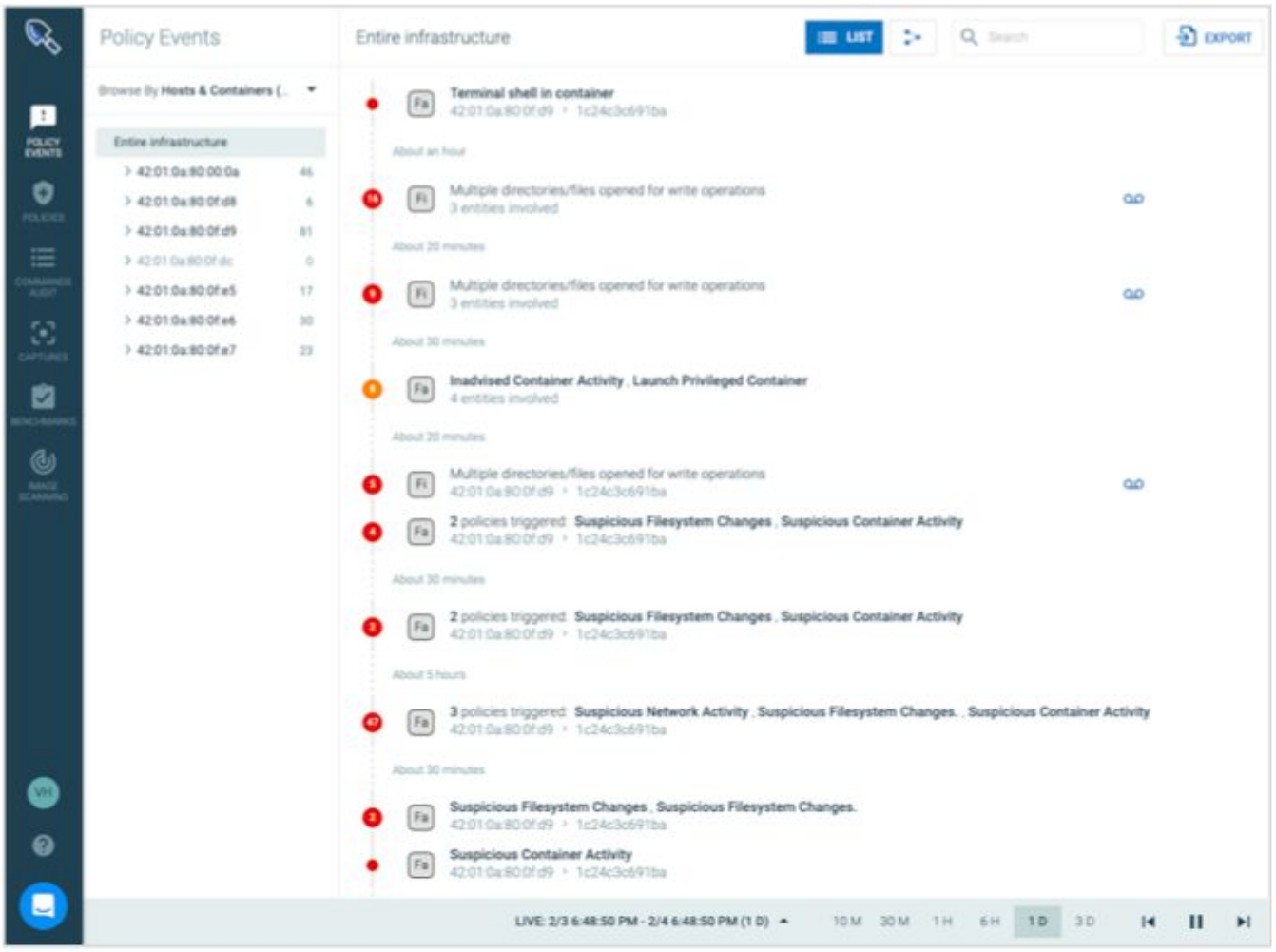
ガイドライン

セキュリティイベント（たとえば、疑わしいまたは異常なアクティビティを識別する通知またはアラート）の日次レビュー、および重要なシステムコンポーネントからのログ、およびファイアウォール、IDS/IPS、ファイル整合性監視などのセキュリティ機能を実行するシステムからのログ(FIM)システムなどは、潜在的な問題を識別するために必要です。「セキュリティイベント」の決定は組織ごとに異なり、技術の種類、デバイスの場所、機能に関する考慮事項が含まれることがあります。 組織は、異常な動作を特定するために、「通常の」トラフィックのベースラインを維持することもできます。

Sysdigがどのように役立つか

Sysdigにアナリストがシステムで発生したすべてのイベントを一目で確認する事のできる複数のサマリーを有しています。

Sysdigイベント概要ダッシュボードには、過去1日間に発生したすべてのイベントが、重大度、ホスト、コンテナー、およびサービスの観点から表示されます。



要件11：

セキュリティシステムとプロセスを定期的にテストを行う

脆弱性は悪意のある個人や研究者によって継続的に発見されており、新しいソフトウェアによって発見されています。システムコンポーネント、プロセス、およびカスタムソフトウェアは、セキュリティ管理が変化する環境を反映し続けることを確認するために頻繁にテストする必要があります。

11.4 トラフィックを監視するためのネットワーク侵入検知/防止

要件の説明

ネットワーク侵入検知システムおよび/または侵入防止システムを使用して、カード会員データ環境のすべてのトラフィックを監視し、疑わしい侵害について担当者に警告します。

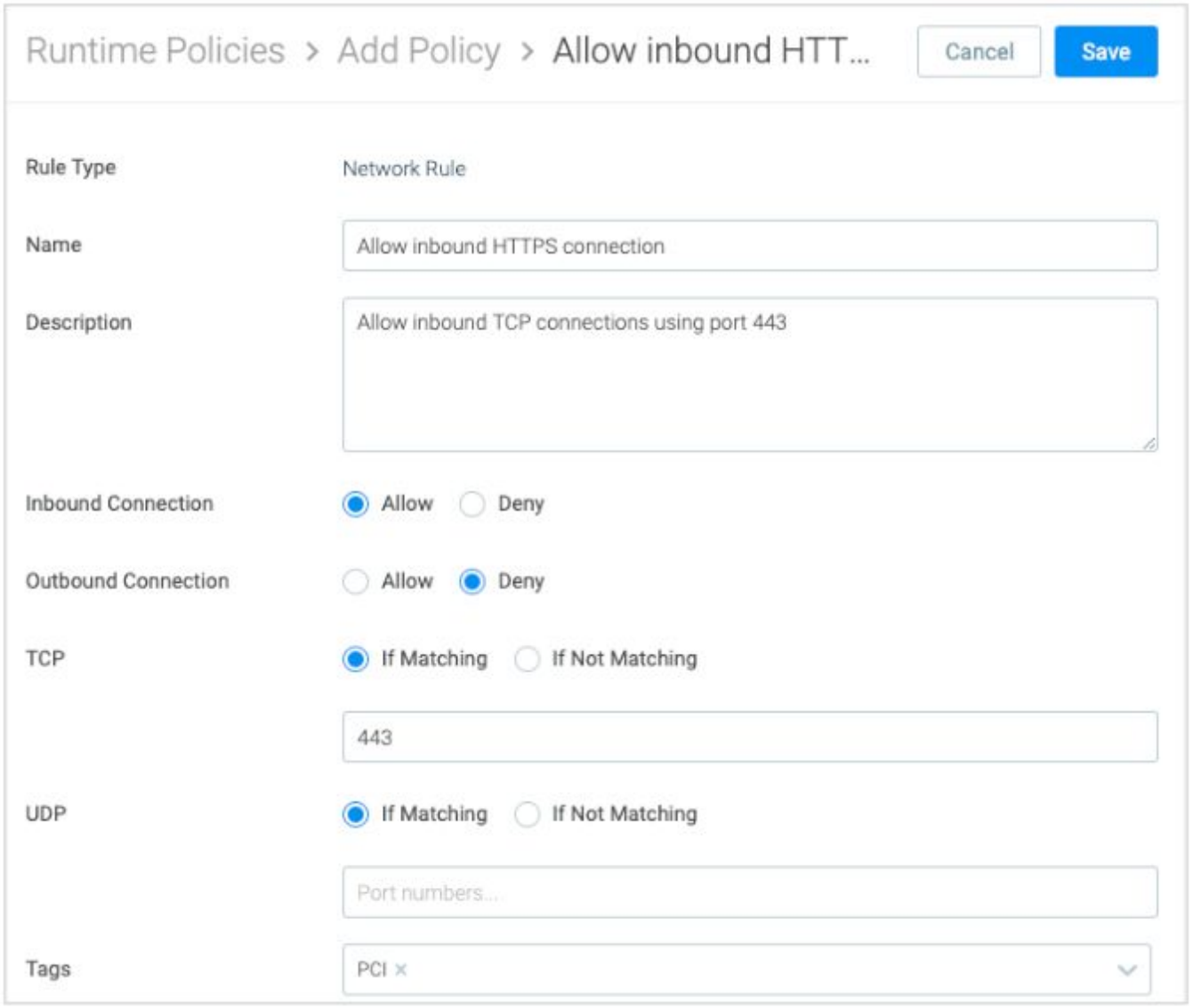
ガイドライン

侵入検知および/または侵入防止技術を使用して、ネットワークへの侵入を検知および/または防止します。カード会員データ環境の境界およびカード会員データ環境の重要なポイントですべてのトラフィックを監視し、疑わしい侵害について担当者に警告します。すべての侵入検知および防止エンジン、ベースライン、シグネチャーを最新の状態に保ちます

Sysdigがどのように役立つか

前のセクションで説明したように、すべてのネットワークアクティビティは、高度なFalcoルールを使用して簡単に監視および検査できます。

また、セキュアネットワークポリシールールを作成して、プロトコル（TCPまたはUDP）、ポート、および方向（着信または発信）に基づいて接続を許可または拒否できます。



11.5.1 変更検出のアラートへの対応

要件の説明

変更検出ソリューションによって生成されたアラートに応答するプロセスを実装します。

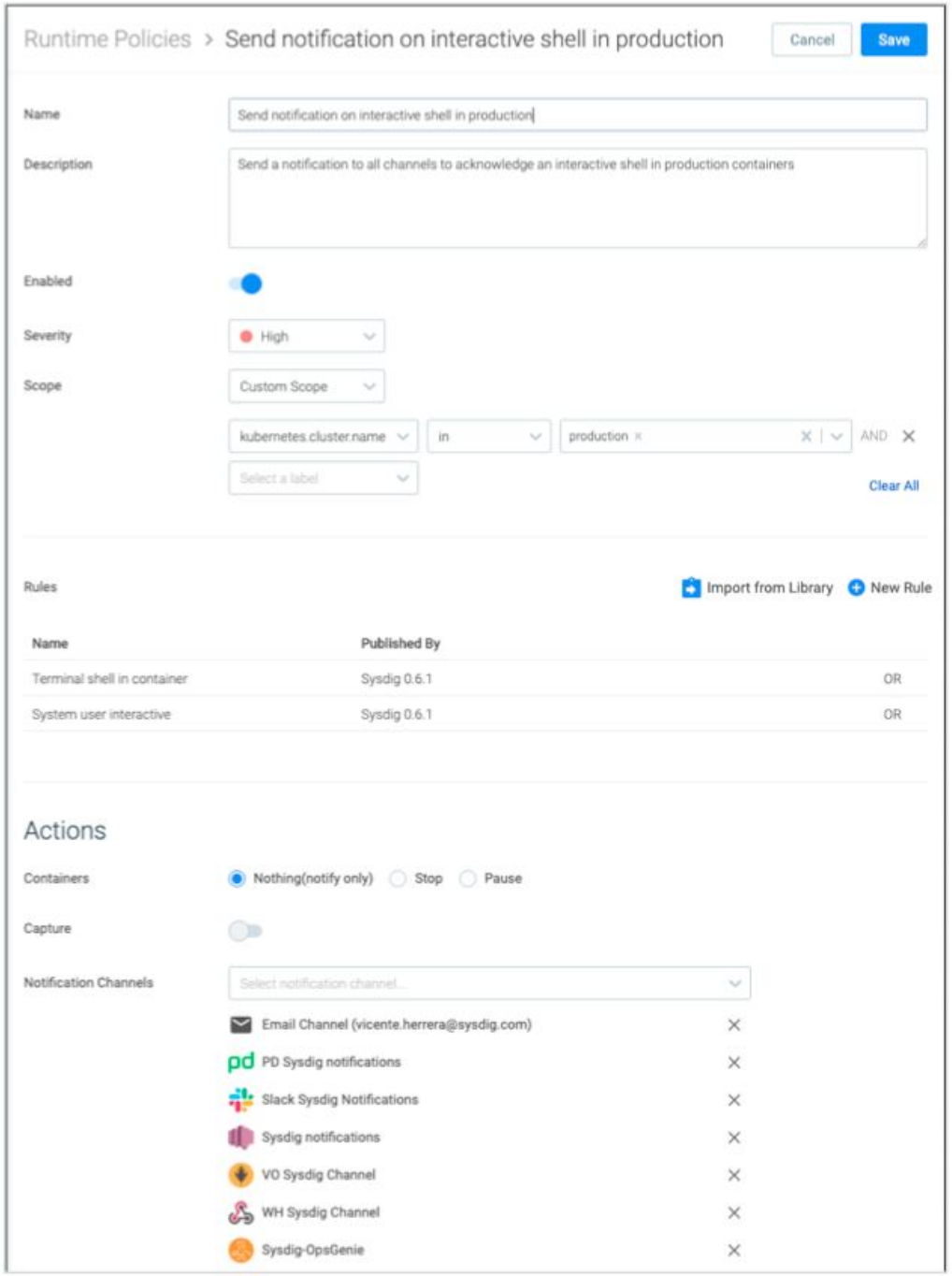
ガイドライン

変更検出メカニズム（ファイル整合性監視ツールなど）を導入して、重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更（変更、追加、削除を含む）を担当者に警告します。 また、少なくとも毎週、重要なファイル比較を実行するようにソフトウェアを構成します

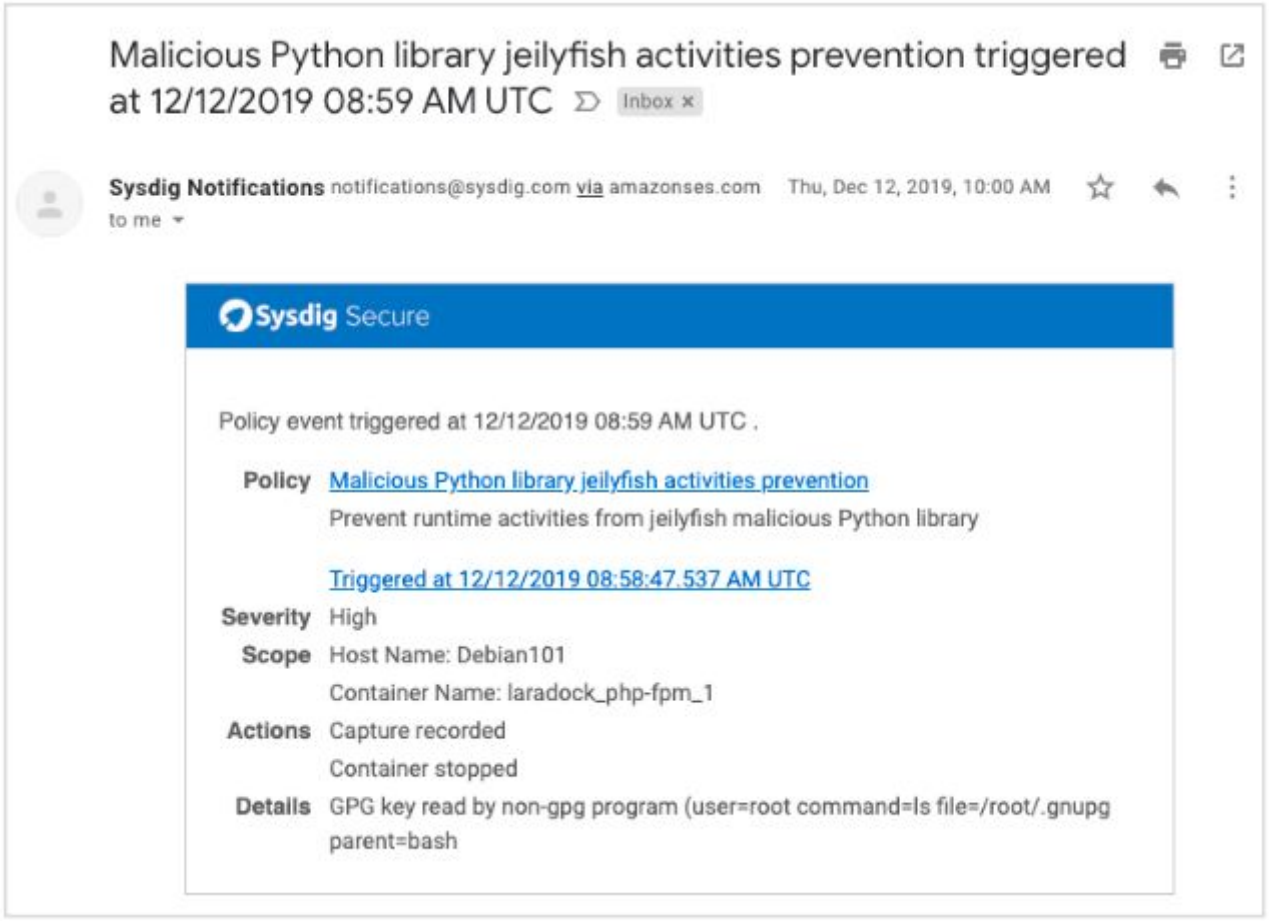
Sysdigがどのように役立つか

すべてのプロセス、ファイル、ネットワーク、コンテナ、システムコールのアクティビティを簡単に監視でき、その後、アラート通知を生成できます。

すべてのポリシーイベントには、イベント検出のアラートを送出する通知チャネルのアクションがあります。



ポリシーイベントの電子メール通知の例



Sysdig Secure DevOps Platformがどのようにあなたとあなたのチームが本番環境でクラウドネイティブアプリを自信を持って稼働させられるかをご覧ください。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。

www.sysdig.jp