

# Sysdig Secure を始めましょう



#### 本文の内容は、Sysdig Secureを始めましょうのドキュメント

(<u>https://docs.sysdig.com/en/getting-started-with-sysdig-secure.html</u>) を元に日本語 に翻訳・再構成した内容となっております。

Sysdig Secureを始めましょう			
Get Started ページ(SaaS)	3		
データソースの接続	4		
エージェントをインストールする	4		
Kubernetes Auditログとの統合	4		
あなたのパイプラインをセキュアにしましょう	4		
あなたのCI/CDパイプラインにスキャニングを統合する	4		
通知チャネルの設定とリンク	5		
リポジトリスキャンアラートのセットアップ	5		
ランタイム環境の保護	5		
ランタイムスキャンアラートのセットアップ	5		
検出ルールの作成	5		
基本的なオンボーディング	6		
Sysdig Secureインターフェースへのアクセス	6		
Sysdig Secureインターフェースの詳細	6		





## Sysdig Secureを始めましょう

#### Get Started $\sim - 2$ (SaaS)

[Get Started]ページは、ユーザーがSysdig Secureを最大限活用できるようするための重要なステップを 把握できるようにします。ユーザーがタスクを完了し、Sysdigが製品に新しい機能を追加すると、ペー ジは新しい手順を案内する内容に更新されます。

	Get Started Let's start improving your security posture.		
POLICIES		~~~	
MMANDS AUDIT	Connect Your Data Sources	Em M	Resources Documentation Systid Secure Release Notes
APTURES	Kubernetes Helm Docker, Linux, Etc.	Sm 🗸	Blog Self Paced Training Support Application Status
	Installing the agent on your infrastructure allows Systig to collect data for monitoring and security purposes. Copy and paste the command below in your cluster. Cluster Name: Cluster Name		(ppp) and (souther
ANNING	AWS_AZURE_GKE curl -s https://download.sysdig.com/stable/install-agent-kubernetes   sudo bash -saccess_key <access_key>collector collector- staging.sysdigcloud.comcollector_port_6666</access_key>	ā	
	OpenShift	-	
	curi -s nttps://download.sysdig.com/stale/install-agent-kupernetes   sudo bash -saccess_key <alless_key>collector collector- staging.sysdigcloud.comcollector_port 6666openshift</alless_key>	U	
	Integrate with the Kubernetes Audit Log	10m >	
	Secure Your Pipeline		
	Integrate Scanning into your CI/CD Pipeline	5m 📏	
	Set up and Link Notification Channel	2m 💙	

[Get Started]ページは、各種情報のリンクページとしても活用いただけます。

- ドキュメント
- リリースノート
- Sysdigブログ
- セルフペーストレーニング
- サポート





ユーザーは、サイドメニューのロケットをクリックして、いつでも[Get Started]ページにアクセスでき ます。

#### データソースの接続

エージェントをインストールする

 インフラストラクチャにエージェントをインストールすると、Sysdigはモニタイングとセキュ リティの目的でデータを収集を始めます

Kubernetes Auditログとの統合

Kubernetes Auditログは、Kubernetes APIアクティビティを記録したセキュリティ関連の時系列のレコードセットを提供します。Kubernetes Auditログを解析することにより、ユーザーアクティビティ、機密性の高い内容の変更、権限の更新を追跡できます。APIログの処理と監査は、Kubernetes環境内での侵害の指標を追跡し、コンプライアンスコントロールを満たすための鍵となります。

#### あなたのパイプラインをセキュアにしましょう

あなたのCI/CDパイプラインにスキャニングを統合する

- CI/CDワーカーノード上でローカルでイメージの分析を可能とする、Sysdigセキュアインライン スキャナは、以下の利点を提供します。
  - イメージがレジストリにプッシュされる前に、イメージをスキャンしてシフトレフトを 実現する
  - スキャンワークロードを並列化および分散する機能
  - 資格情報をSysdigのSaaSサービスに記録したり、分析のためにSysdigバックエンドにイメージを送信する必要もありません。





#### 通知チャネルの設定とリンク

 Sysdig Secureはアラートを発行して、イベント、異常、または注意が必要なセキュリティイン シデントのプロアクティブな通知を行います。アラートシステムは、通常の電子メール、Slack 、クラウドプロバイダーの通知キュー、カスタムWebhookなど様々なプッシュゲートウェイを 提供します。

リポジトリスキャンアラートのセットアップ

 スキャン結果をSysdigが提供する通知チャネルのいずれかと統合することにより、ユーザーは イメージ分析プロセスの出力に関するレポートをすぐに実行できます。リポジトリアラート は、レジストリ/リポジトリスコープに応じて異なるトリガー条件を使用してカスタマイズでき ます。

#### ランタイム環境の保護

ランタイムスキャンアラートのセットアップ

ユーザーがセットアップできる最も実用的なアラートの1つは、既存のランタイムイメージが新しく発見された脆弱性の影響を受けているかどうかを検出することです。これらのアラートは、コンテナおよびKubernetesメタデータを使用して範囲を設定できるため、イメージがコンプライアンスから外れるとすぐに適切なチームに通知されます。

検出ルールの作成

Sysdig Secureは、オープンソースプロジェクトであるFalcoの上に構築されたビヘイビア検出エンジンを活用して、異常なランタイムアクティビティを検出して対応できます。さらに、ユーザーは、基本ポリシーエンジンを使用して、プロセス実行、ファイルアクセス、およびネットワークアクティビティのホワイトリストベースのセキュリティルールを簡単に作成できます。





### 基本的なオンボーディング

このセクションでは、Sysdig Secure(オンプレミス)のオンボーディングの秘訣について説明しま す。

Sysdig Secureインターフェースへのアクセス

Sysdig Secureインターフェースにアクセスするには、Welcome Wizardで、Sysdigエージェントをイン ストールし、コア管理ユーザーを作成する必要があります。インストール手順については、エージェ ントインストールドキュメントをご参照ください。

注記

ユーザーを追加するには、Sysdig Secureまたは統合認証ツールのいずれかを使用して、ユーザー資格情報も定義する必要があります。ユーザー作成の詳細については、ユーザーおよびチーム管理ドキュメントをご参照ください。

Sysdig Secureインターフェースの詳細

Sysdig Secure UIは、以下のモジュールで構成されています。





Runtime Policies				
Q High	Medium Low Info			
•	Create/Modify Configmap With Private Cr Entire Infrastructure	Updated 19 days ago 1 rules   Notify Only		
•	Ingress Object Without TLS Cert Created Entire Infrastructure	Updated 2 months ago 1 rules   Notify Only		l
•	Launch Suspicious Network Tool in Contai Entire Infrastructure	Updated 2 months ago 1 rules   Notify Only		ļ
•	Unexpected outbound connection destina Entire Infrastructure	Updated 22 days ago 1 rules   Notify Only		
•	Baselining profile - Sysdig/agent container.image.id = "ecb00980057a702652f118	Updated 2 months ago 6 rules   Notify Only		
•	Sensitive Info Exfiltration kubernetes.namespace.name = "ping"	Updated 2 months ago 1 rules   Notify Only   Capture 25 secs		
•	Terminal shell in container kubernetes.deployment.name = 'woocommerce'	Updated 2 months ago 1 rules   Notify Only   Capture 30 secs		
0	All K8s Object Modifications Entire Infrastructure	Updated 2 months ago 8 rules   Notify Only		
0	Suspicious K8s Activity Entire Infrastructure	Updated 2 months ago 1 rules   Notify Only	6:	
	Runtime Q High O O O O O O O O O O O O O O O O O O O	Runtime Policies         Q       High       Medium       Low       Info         •       Create/Modify Configmap With Private Cr Entire Infrastructure       •       •         •       Ingress Object Without TLS Cert Created Entire Infrastructure       •       •         •       Launch Suspicious Network Tool in Contail. Entire Infrastructure       •         •       Unexpected outbound connection destina Entire Infrastructure       •         •       Baselining profile - Sysdig/agent container.image.id = 'ecb00980057a702652f118         •       Sensitive Info Exfiltration kubernetes namespace name = 'ping'         •       Terminal shell in container kubernetes.deployment.name = 'woocommerce'         •       All KBs Object Modifications Entire Infrastructure         •       Suspicious K8s Activity Entire Infrastructure	Runtime Policies         Q       High       Medium       Low       Info         •       Create/Modify Configmap With Private Cr       Updated 19 days ago       1 rules   Notify Only         •       •       Entire Infrastructure       Updated 2 months ago         •       •       Ingress Object Without TLS Cert Created       Updated 2 months ago         •       •       Entire Infrastructure       Updated 2 days ago         •       •       Entire Infrastructure       Updated 2 months ago         •       •       Baselining profile - Sysdig/agent       Updated 2 months ago         •       •       Baselining profile - Sysdig/agent       Updated 2 months ago         •       •       Sensitive Info Exfiltration       Updated 2 months ago         •       •       Sensitive Info Exfiltration       Updated 2 months ago         •       •       Trues   Notify Only   Capture 25 secs       •         •       •       Trues   Notify Only   Capture 30 secs       •	Runtime Policies       Add Policy         Image: High Medium Low Info       Image: Notify Only         Image: Create/Modify Configmap With Private Cr. Indes Notify Only       Updated 19 days ago         Image: Notify Only       Indes Notify Only         Image: Notify Only       Image: Notify Only

- ポリシーイベント
- <u>ポリシー</u>
- 「ベータ」アクティビティ監査
- <u>キャプチャ</u>
- イメージスキャン
- ベンチマーク

ワークフローの好みや、Sysdig Secureの実装、もしくは、新規ユーザかの状況に応じていくつかのスタートポイントがあります。

- 新しいSysdig Secure環境の場合は、ポリシーモジュールに移動して、環境に必要なポリシーとルールの構成を開始します。
- 新しいSysdig Secureユーザーの場合、ポリシーイベントモジュールに移動して、環境の 現在の状態を確認します。

