sysdig

CHECKLIST

SysdigとWizを徹底比較

ランタイムインサイトを活用したリアルタイムクラウドセキュリティにより包括的な可視性を実現

魅力的なユーザーインターフェースに惑わされてはいけません。Wizのようなツールには、使用中、つまり実行環境で使用されているものを包括的に理解する能力が欠けているようです。そのため、適切なリスクの優先順位付けや、ランタイムコンテキストに基づいて行える修正に関して課題が残ります。また、Wizには、脆弱性を効果的に優先順位付けするために必要となるランタイムコンテキストが不足しているため、クラウドやコンテナへの脅威の特定や対応に苦慮することになりそうです。

Sysdigが選ばれる理由

Sysdigは、ランタイムインサイトを活用することで脅威をリアルタイムに検知し、リッチなコンテキストを表面化することにより即座に脅威に対応します。この独自のランタイムの可視性により、Sysdigは2秒以内に脅威を検知できるほか、使用中のものだけを表示するフィルタ機能を通じて脆弱性のノイズを95%削減できます。Wizには、このようなランタイムの可視性が欠けているため、最も重大なリスクに優先順位を付けて対処することはできないようです。

Sysdigを使うと、次のことが可能となります。

- リアルタイムの検知とランタイムインサイトにより、リスクの優先順位を決定
- クラウド環境における包括的なエンドツーエンドのセキュリティを実現
- ランタイムインサイトを活用したクラウド攻撃グラフの活用

SysdigとWizの比較

下記に示すチェックリストでは、SysdigとWizのコンテナとクラウドのセキュリティにおけるCNAPP機能を比較しています。

01 優れたユーザー体験とエンタープライズグレードの機能

機能	sysdig	Wiz
統合型セキュリティダッシュボード。これにより、クラウド、コンテナ、Kubernetesクラスタ、サードパーティアプリ、コードレポジトリにまたがるリスクを可視化できます。	✓	◐
簡素化されたエージェントレスのクラウドオンボーディング。これにより、チームが即座にセキュリティリスクを評価して対処できるようになります。	✓	✓
オープンスタンダード（FalcoやOPAなど）に基づいて構築された、柔軟に設定可能で透明性の高いプラットフォーム。	✓	✗
API/CLIファーストのプラットフォーム。サードパーティのツール、プロセス、プラットフォーム（SIEM、CI/CD、ITSM、ポケットベルなど）と統合できます。	✓	◐
エンタープライズスケールに対応。	✓	◐
カーネルモジュールとeBPFを利用したインスツルメンテーションのオプション。これにより、ランタイムの可視性を損なうことなく、柔軟なデプロイメントが可能となります。	✓	✗
ロールベースのアクセス制御（RBAC）と、ゾーンによるリソースのグルーピングを使って、きめ細かな責任の割り当てを実施できます。	✓	✓
SAMLのサポートを伴うシングルサインオン（SSO）。これにより、制御されたシームレスな認証を実現できます。	✓	✓

02 脆弱性管理

機能	sysdig	Wiz
コンテナイメージ。レジストリ、CI/CDパイプライン、実行時（サーバーレスコンテナを含む）における脆弱性をスキャンできます。	✓	◐
リスクベースの脆弱性ポリシー。脆弱性のスコアリング、イメージの設定ミス、シークレットの検知をカバーします。	✓	◐
スケジュールされたオンデマンドのイベントトリガ型のイメージ再チェック。これにより、脆弱性の盲点を回避できます。	✓	◐
外部CVEフィードとの統合。これにより、業界で検証済みの脆弱性評価を提供できます。	✓	✓
使用中のパッケージに基づく脆弱性の優先順位付け。	✓	◐
脆弱性の優先順位付けフィルタとレポーティングの強化。これには、修正の有無や悪用可能性などが含まれます。	✓	✓
ホストの脆弱性管理のためのエージェントベースおよびエージェントレススキャンオプション。	✓	◐

03 クラウドの検知と対応

機能	sysdig	Wiz
ホスト、コンテナ、Kubernetes、クラウド、およびサードパーティアプリ（OktaやGitHubなど）全体を通じて脅威を検知できるような、統一的なポリシー言語。	✓	✗
脅威リサーチャーによって更新とキュレーションが行われるマネージド型の検知および対応ルール。	✓	✗
コンプライアンスの枠組みや攻撃戦術のタグ付け(SOC2、PCI、HIPAA、CIS、MITREなど)を標準でサポートする検知ルール。	✓	◐
クラウド環境における攻撃に関する最も深いレベルの可視性。これには、拡張プロセスツリーによるコンテキストのリッチ化と、より広いコンテキストに基づくイベントの相互関連付けが含まれます。	✓	✗
拡張されたFIM機能。これにより、ホスト、コンテナのファイルシステム、およびメモリ全体における、ファイルベースの攻撃とファイルレス型の攻撃の両方をリアルタイムで検知できます。	✓	✗
多層型のアプローチ。これは、機械学習、ドリフト防止、およびイメージプロファイリングを、Falcoベースの検知ポリシーと組み合わせたものです。	✓	✗
疑わしいワークロードに入って調査するためのRapid Responseシェル。インフラストラクチャーとワークロードのライブマッピングから得られたMITRE ATT&CKのコンテキストに基づいて、疑わしさを判断しています。	✓	✗
インシデント対応チームやフォレンジックチーム向けの詳細かつ実用的なデータの取得。これにより、セキュリティ監査や根本原因の分析が可能となります。	✓	✗

04 クラウドセキュリティポスチャー管理 (CSPM)

機能	sysdig	Wiz
スナップショットを介したエージェントレス型のクラウドスキャン。	✓	✓
自動化されたGitOpsプルリクエストにより、IaCソースにおける安全でないクラウドデプロイメントを修復。	✓	✗
正確なMITREリスクマッピングによって強化された、業界ベンチマークと規制コンプライアンスフレームワークをサポートするコンプライアンスレポート。	✓	✓
特定のポリシーやクラウド資産に関する、より低リスクの違反を管理下で受け入れること。柔軟な修復計画を立てることができます。	✓	◐
リスクの特定、ランク付け、対処を行うためのリスクの優先順位付け。これは、静的なポスチャーや脆弱性のチェックを、使用中の脆弱性、アクセス許可、アクティブな脅威から得られた実行時のコンテキストと組み合わせることで実施されます。	✓	◐
リスクに関する明確な視覚的表示の提供。これは、アクティブなイベントと脆弱性や設定ミスを重ね合わせた攻撃グラフを通じて実施されるものであり、これにより、予防と対応の両方のシナリオにおいて完全な状況認識が可能となります。	✓	◐
IaCから本番環境に至るまでの資産を追跡する統一されたクラウド資産インベントリ。これにより、パブリックエクスポージャー、使用中のパッケージ、制御の失敗などのランタイムインサイトをフィルタリングできます。	✓	◐

05 権限およびエンタイトルメント管理（CIEM）

機能	sysdig	Wiz
基本的なユーザーアカウントとロールのセキュリティ衛生。これは、リスクのあるユーザープロファイル設定を特定することにより実施されます。	✓	✓
アカウントとロールに関する簡素化されたポスチャー強化。これは、推奨されるIAMポリシーに基づく、過剰なパーミッションのガイド付き修復を通じて実施されます。	✓	✓
最小権限の原則の適用。これは、使用中の権限の分析に基づいて実施されます。	✓	✗

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

Sysdig. Secure Every Second.

詳細は、**sysdig.jp**をご覧ください。

デモを依頼 →

sysdig