Carbon Black Container ユーザー ガイド

2023 年 9 月 26 日

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
〒 108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

目次

VMware Carbon Black Container ユーザー ガイド

VMware Carbon Black Container™ は、可視性、セキュリティ強化、脆弱性管理、ランタイム保護機能を提供することで、オンプレミスとクラウドネイティブの両方のワークロードに対応する包括的なセキュリティ ソリューションです。

Carbon Black Container は、ワークロードを強化するために脆弱性と構成ミスを特定することで、リスクを軽減するのに役立ちます。

このソリューションは、セキュリティ チームに対して、既存の DevOps プロセスに統合しながらコンプライアンスを適用する可視性と機能を提供します。VMware Carbon Black により、組織は大規模な Kubernetes 環境のリスクを軽減し、コンプライアンスを維持し、セキュリティを簡素化できます。

対象ユーザー

Carbon Black Container は、セキュリティ チームと DevOps チームの両方向けです。セキュリティの移行が進むにつれて、開発者はセキュリティの所有権を高め、最新のアプリケーション ライフサイクルのコードとビルド ステージを通じてセキュリティ対策を実施する必要があります。

セキュリティ チームは、展開ステージとランタイム ステージでコンプライアンス要件を適用し、アプリケーションを安全に保つ必要があります。

このガイドは、セキュリティ アナリスト、DevSecOps、および DevOps チーム向けに記述されています。コンテナと Kubernetes クラスタに関する知識があることを前提としています。

Carbon Black Container の概要

1

Carbon Black Container ソリューションは、DevOps チームとセキュリティ チームが Kubernetes クラスタと展開されたアプリケーションの安全を確保するために必要な可視性と制御を提供できます。このトピックでは、Carbon Black Container のメリットの概要を確認できます。

VMware Carbon Black Container Essentials および VMware Carbon Black Container Advanced

Carbon Black には、次の表に記載されている 2 つの Carbon Black Container パッケージが用意されています。

VMware Carbon Black Container Essentials	VMware Carbon Black Container Advanced
セキュリティ状態のダッシュボード	Container Essentials +
遵守ポリシーの自動化	脅威検出
優先リスク評価	アノマリ検知
ガバナンス制御と適用	出力方向セキュリティ
イメージ スキャンと脆弱性管理	SIEM 統合
CI/CD セキュリティ強化によるシフトレフト セキュリティ	
トポロジ マップ	
自動適用	

概要

Carbon Black Container は、Kubernetes クラスタに展開されたすべてのワークロードに、ポリシーベースのレポートを提供し、組織のセキュリティ状態を適用します。

Carbon Black Container を使用すると、次のことを実行できます。

- Kubernetes アプリケーションのライフサイクル全体を保護します。
- 展開前に脆弱性と構成ミスを検出して修正します。
- コンプライアンス基準を満たします。
- シンプルでセキュアなマルチクラウドとハイブリッド クラウドの Kubernetes を規模を拡大して実現します。

ユースケース

- Kubernetes Security Posture Management (KSPM)
- コンテナ イメージのスキャン
- コンテナ イメージの強化
- Kubernetes 環境の可視性を向上した
- セキュリティ コンプライアンス、ガバナンス、および適用を確保した
- アノマリを特定してアラートを送信するアプリケーションの動作モデルを構築する
- コンテナと Kubernetes アプリケーションを保護する
- Kubernetes 環境の可視性を向上させる

DevOps チームの主なメリット

- 迅速かつ簡単な展開
- CI/CD パイプラインと既存のプロセスとのシームレスな統合
- ビルド時の脆弱性と構成ミスへの対処
- セキュリティを損なうことな迅速な配信を実現
- クラスタ内ネットワークの可視性マップを使用して、アプリケーションの接続と構成を可視化
- 実行時のコンテナ イメージのリスク優先脆弱性評価
- Kubernetes でのシークレット管理の構成ミスを理解する

セキュリティ チームの主なメリット

- Kubernetes のセキュリティ状態を完全に可視化
- 優先脆弱性レポートの有効化
- セキュリティ ポリシーの定義とカスタマイズ
- 開発者がビルド時に脆弱性や構成ミスに対処できるようにする
- セキュリティを損なうことな迅速な配信を実現
- イメージの脆弱性を特定の実行中のワークロードに接続する
- プライベートおよびパブリックの宛先への出力方向接続を保護する
- IP レピュテーションを使用して悪意のある出力方向接続を特定する
- 機械学習と AI を使用してワークロードのネットワーク動作モデルを構築する
- 悪意のあるネットワーク アクティビティを特定する
- イベントとアラートを 1 つのダッシュボードに統合する

- Kubernetes クラスタ、ネットワーク フロー、アプリケーション アーキテクチャの可視化

次のトピックを参照してください。

- コンテナのセキュリティを展開する理由
- Carbon Black Secures コンテナの機能
- コンテナ アーキテクチャ
- コンテナの概念と用語

コンテナのセキュリティを展開する理由

セキュリティを DevOps プロセスに統合することで、Carbon Black Container を使用して高品質アプリをすばやく簡単に展開できます。開発の早い段階でアプリを保護すると、本番環境の脆弱性を軽減します。

コンテナ セキュリティは、包括的なセキュリティ評価の重要な部分です。これは、セキュリティ ツールとポリシーの組み合わせを使用して、コンテナ化されたアプリケーションを潜在的なリスクから保護する方法です。コンテナ セキュリティは、ソフトウェア サプライ チェーンや CI/CD パイプライン、インフラストラクチャ、コンテナ ランタイム、コンテナで実行されるライフサイクル管理アプリケーションのあらゆる側面を含む、環境全体のリスクを管理します。

開発から本番環境までの統一されたセキュリティ戦略は、開発の早い段階で脆弱性や構成ミスを検出し、コンテナがもたらす攻撃対象を最小限に抑えるために重要です。ビルド フェーズから開始することで、DevOps チームとセキュリティ チームは設計上安全なワークロードを作成できます。これらのチームは、Kubernetes クラスタとそのアプリケーションを保護するために、ランタイム レイヤーでワークロードを可視化する必要があります。

攻撃から効果的に保護するには、開発ライフサイクルを通じて各レイヤーでセキュリティを統合する必要があります。ますます複雑化する環境で脅威に対処するには、アプリケーションのライフサイクル全体にわたる多層的なアプローチが必要です。

Kubernetes を採用する組織は、脆弱性や構成ミスを回避するために、セキュリティ チームには可視性を提供し、開発チームには構成とコンプライアンス ポリシーを使用してガードレールを設定する必要があります。これらのポリシーにより、安定したガバナンスを確保し DevOps ワークフローの中断を最小限に抑え、ビジネスの機敏性と市場化までの時間に影響を与えることなく、展開ライフサイクル全体を保護します。

Carbon Black Secures コンテナの機能

Carbon Black Container は、すべてのワークロードを可視化し、コンプライアンス、セキュリティ、ガバナンスを 1 つのダッシュボードから適用する機能を提供します。

Carbon Black Container は、開発から本番環境まで DevOps のスピードで、エンタープライズグレードのコンテナ セキュリティを実現します。このソリューションにより、DevOps チームとセキュリティ チームは、既存のアプリケーション ビルドと展開プロセスに統合しながら、詳細な可視性、コンテキスト、コンプライアンスを適用する機能を得ます。Carbon Black Container により、あらゆる規模の組織が大きな規模で Kubernetes 環境のリスクを低減し、コンプライアンスを維持し、セキュリティを簡素化できます。

Kubernetes セキュリティ状態の可視化

Carbon Black Container により、セキュリティ チームと DevOps チームは Kubernetes 環境を完全に可視化し、ワークロードをプロアクティブに強化し、脆弱性や構成ミスがもたらすリスクをより正確に把握し、低減することができます。組織は、イメージ リポジトリを使用してイメージに関連するリスクを調査し、その脆弱性を実行中のワークロードに直接関連付けることができます。

セキュリティ状態のダッシュボード

単一の管理画面で、以下を含む Kubernetes クラスタまたはアプリケーション全体のセキュリティ状態を完全に可視化できます。

- Kubernetes クラスタとワークロード インベントリの可視性。
- すべての脆弱性、構成ミス、ルール違反の複合ビュー。
- 修正に優先順位を付けるために、すべてのワークロード属性について集計された統合リスク スコア。

ネットワーク マップ

ネットワーク可視性マップを使用すると、アプリケーション アーキテクチャの単一のマップでワークロード接続を表示できます。ネットワーク可視化マップは、アプリケーション アーキテクチャとネットワーク トラフィックの動作をよりよく理解するための詳細情報とコンテキストを提供します。

アプリケーションのクリーン ビューを取得するには、フィルタを使用してマップの接続を許可し、システム名前空間などの不要なノイズを削除できます。同様のフィルタを使用して、どの接続が暗号化されているか暗号化されていないかを把握して、アプリケーション トラフィックの状態を完全に可視化できます。ネットワークの可視性マップの目的は、Kubernetes クラスタにインストールされているアプリケーションの接続と構成についてチームがよりよく理解できるようにすることです。

Kubernetes アプリケーションのライフサイクル全体の保護

Carbon Black Container は開発者ライフサイクルに統合され、本番環境に展開される前にアプリケーションのリスクを分析および制御します。

この専用ソリューションは DevSecOps を自動化し、Kubernetes で実行されているワークロードのライフサイクル全体にクラウド ネイティブの継続的なセキュリティとコンプライアンスを提供します。

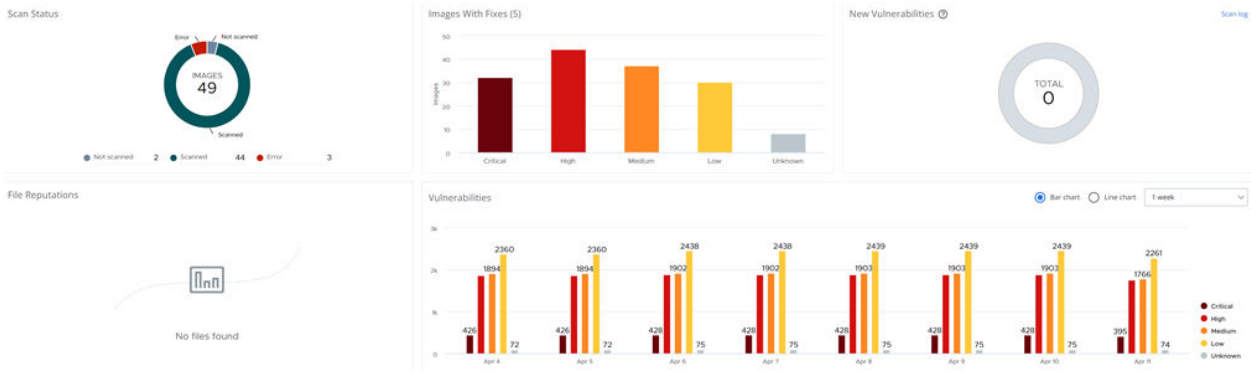
- CI/CD パイプラインと統合します。
- ビルドおよび実行時の脆弱性についてコンテナ イメージをスキャンします。
- コンテンツベースのセキュリティ ポリシーを迅速かつ簡単に作成および適用します。
- セキュリティ ポリシーと制御をカスタマイズおよび自動化して、目的の状態を強化し、構成エラーを回避します。
- Kubernetes クラスタに展開されたすべてのワークロードに対して、セキュリティ状態のレポートと適用を有効にします。

ランタイム クラスタ スキャンの自動化

CI/CD 統合とシフトレフト アプローチは効果的な戦略です。ただし、本番環境でセキュリティ状態を継続的に監視することも必要です。

クラスタ スキャンは、CI/CD で開発されたアプリケーションをサードパーティのコンポーネントおよびインフラストラクチャ レベルのコンポーネントにスキャンする場合と同じレベルの可視性を提供します。実行中のワークロードで使用されるコンテナ イメージが最新で、脆弱性を検出できることを確認することが重要です。

ランタイム クラスタ スキャンを使用すると、実行中のすべてのイメージの構成ミスと脆弱性をスキャンして、全体的なリスクをより適切に評価できます。たとえば、適用された構成とマニフェストがポリシーと一致していることを確認し、脆弱な構成ミスを特定し、クラスタ自体にクリア テキスト シークレットや悪意のあるコンテナが実行されていないことを確認します。この機能により、DevOps チームとセキュリティ チームは実行状態のセキュリティ レベルを理解し、ワークロードのセキュリティを強化するためにパイプラインに必要な変更を加えることができます。



コンテナ イメージには、いくつかのセキュリティ上の課題があります。イメージは通常、他のイメージを階層化することで構築されますが、そのイメージには脆弱性が含まれている可能性があり、その脆弱性が本番システムに入り込んでしまうことがあります。欠陥やマルウェアもコンテナ イメージに影響を与える可能性があります。コンテナの実績が不明な場合、これらのリスクは増加します。

次の機能を持つコンテナ イメージ レジストリは、これらのリスクを軽減できます。

- 共通脆弱性識別子 (CVE) データベースにある脆弱性のイメージをスキャンします。
- 公証を使用して、イメージに既知および信頼済みとして署名します。
- レジストリに接続するためのセキュアで暗号化されたチャネルを設定します。
- ユーザーを認証し、Active Directory などの標準ディレクトリ サービスで管理されている既存のエンタープライズ アカウントを使用してアクセスを制御します。
- 最小権限と職務の分離の原則を使用して、レジストリへのアクセスを厳密に制御します。
- 脆弱性に対する組織のしきい値を満たすイメージのみをユーザーが使用できるようにするポリシーを作成します。

脆弱性スキャン

ほとんどのアプリケーションは、サードパーティのイメージ レジストリをソースとするコンポーネントを使用します。これを認識した攻撃者は、多くの場合、これらのレジストリに悪意のあるコードを挿入します。コンテナは、多くの場合、DockerHub などのパブリック イメージ リポジトリから Ubuntu や CentOS などのオペレーティング システムの基本イメージを使用します。オペレーティング システムのパッケージとその上のアプリケーションには、脆弱性が含まれている可能性があります。

脆弱性スキャンは、既知の脆弱性を検出してセキュリティ侵害のリスクを軽減するのに役立ちます。イメージ上のイメージの脆弱性またはマルウェアを特定し、それらを本番環境に移行しないようにすることで、コンテナ化されたアプリケーションの攻撃対象を減らすことができます。

コンプライアンスとポリシーの自動化を有効にする

このコンテキストで、コンプライアンスとは、CIS ベンチマークや独自の組織要件などの業界標準を指します。通常、SecOps チームは組織のセキュリティ ポリシーを定義し、DevOps チームはポリシーを作成してコンプライアンスを確保します。

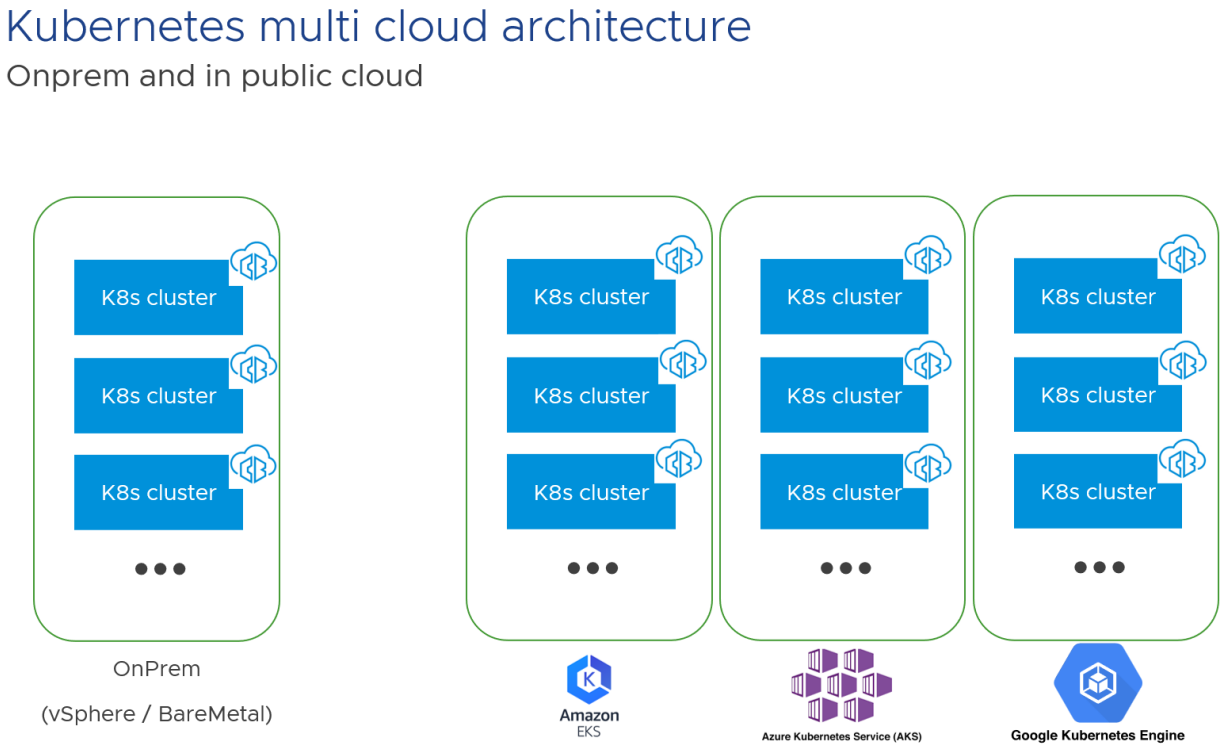
Carbon Black Container ソリューションのコンプライアンスとポリシーの自動化機能:

- 開発サイクルに移行して、ビルドの脆弱性を検出して防止します。
- 自動ポリシーを作成して、安全な構成を適用します。
- 組織の要件および CIS ベンチマークなどの業界標準に準拠していることを確認します。
- 事前に作成されたテンプレートとカスタマイズされたポリシーを活用します。

コンテナ アーキテクチャ

このトピックでは、Carbon Black Container と Kubernetes アーキテクチャについて説明します。

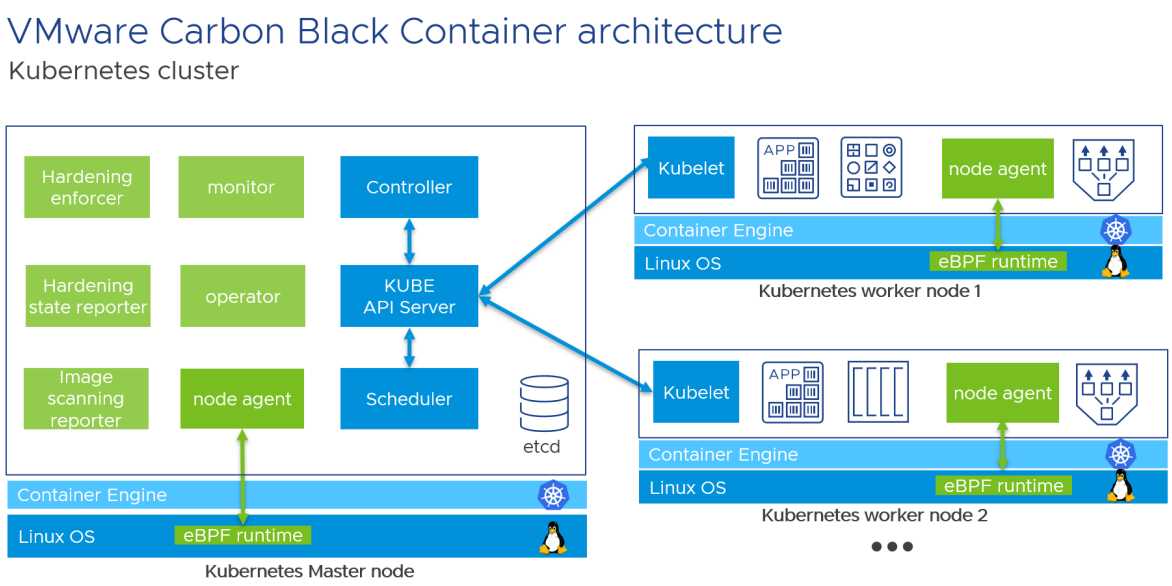
Carbon Black Cloud は、クラウドネイティブな SAAS ソリューションです。オンプレミスおよびパブリック クラウド（Amazon EKS、Azure Kubernetes サービス、Google Kubernetes エンジン）で複数の Kubernetes クラスタを保護できます。



Kubernetes クラスタ コンポーネント

Kubernetes クラスタで、Carbon Black Container は相互に通信する主要コンポーネントで構成されます。

すべての Carbon Black Container ポッドは、cbcontainers-dataplane と呼ばれる専用の名前空間で実行されます。ポッドはすべて、直接接続またはプロキシを介して Carbon Black Cloud に接続する必要があります。



前の図では、すべての Carbon Black Cloud コンポーネントが緑色で表示され、すべての Kubernetes コンポーネントが青色で表示されています。

Carbon Black Container は、eBPF テクノロジー（外部リンク）を使用して、Linux でランタイム セキュリティ レイヤーを追加します。eBPF は、カーネル ソース コードの変更やカーネル モジュールのロードを必要とすることなく、カーネル機能を安全かつ効率的に拡張します。Carbon Black は、すべての Linux カーネル バージョン 4.4 以降で Carbon Black Container の eBPF を使用します。eBPF を使用すると、Carbon Black Container はすべての入力方向、出力方向、内部ネットワーク接続を監視できます。eBPF は、ポートのスキャン、アノマリな動作、悪意のある IP アドレスおよび URL への接続を検出します。

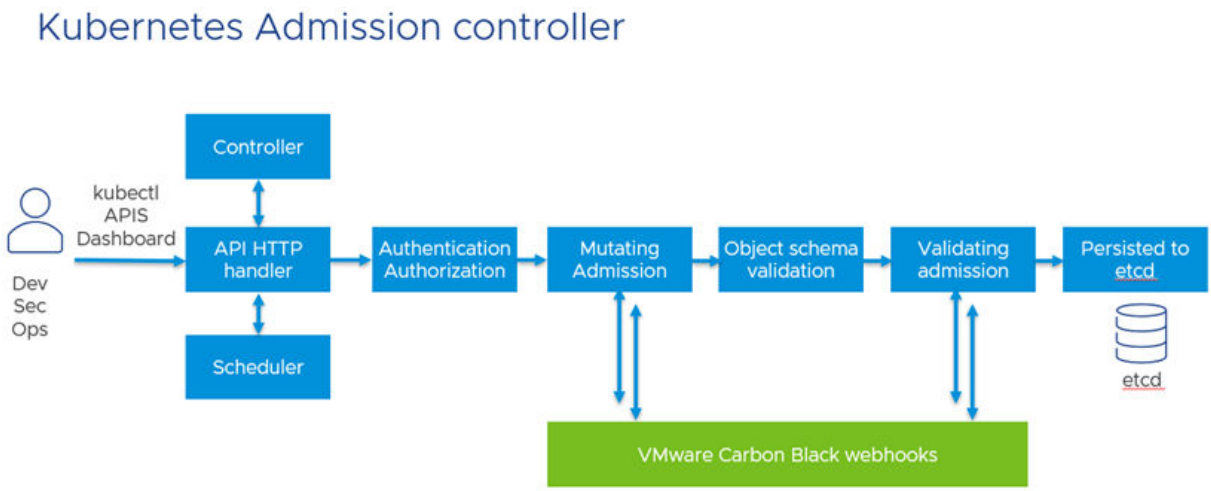
ノード エージェント ポッドは Kubernetes DaemonSet です。これにより、すべてのノードがこのポッドのコピーを実行します。そのため、Kubernetes クラスタにノードを追加でき、Carbon Black は自動的にそれらを保護します。各ワーカー ノードに 1 つのノード エージェントが存在します。Daemonset は、通常、監視、ネットワーク、セキュリティ ソリューションに使用されます。このテクノロジーは、すべての Kubernetes で使用できます。

Kubernetes アドミッション コントローラ

VMware Carbon Black Container には、次の 2 種類のポリシーがあります。

- ランタイム ポリシー
- セキュリティ強化ポリシー

セキュリティ強化ポリシーには、Kubernetes クラスタの アドミッション コントロール（外部リンク）を拡張できる Webhook が含まれます。Carbon Black Container は、管理者が Carbon Black Container セキュリティ強化ポリシーに準拠していないリソースを展開すると、自動的に適用（または変更）、ブロック、またはアラートを実行できます。



コンテナの概念と用語

このトピックでは、概念を紹介し、Carbon Black Container で使用される一般的な用語を定義します。

一般的な専門用語

用語	定義
アドミッション コントローラ	Kubernetes API サーバへの要求を妨害するコードの一部。アドミッション コントローラは、オブジェクトの作成、削除、または変更の要求を制限します。
cbctl	Carbon Black Cloud コンテナと Kubernetes ワークロードのセキュリティを制御できるコマンドライン ツール。Carbon Black Cloud CLI クライアントはコンテナ イメージをスキャンし、その健全性を Carbon Black Cloud コンソールに報告します。
共通脆弱性識別子 (CVE)	一般に知られている情報セキュリティの脆弱性と識別子のための参照方法。
コンテナ	軽量でポータブルな実行可能イメージ。コンテナを使用すると、同じオペレーティング システム (カーネル) インスタンスで複数のアプリケーション ランタイム環境を仮想化できます。
コンテナ オーケストレーション	API とインターフェイスを公開します。コンテナ ライフサイクルの管理に役立ちます。
制御プレーン	ワーカー ノードとポッドを管理します。
コントローラ	クラスタの状態を監視し、必要に応じて変更を行ったり、要求したりします。各コントローラは、現在のクラスタの状態を目的の状態に近づけようとします。
クラスタ	ノードのセット。各クラスタには、少なくとも 1 つのノードが含まれています。

用語	定義
DaemonSet	すべてのノードがこのポッドのコピーを実行することを保証するポッド内のノード エージェント ポッド。このノードを使用すると、ポッドにノードを追加し、Carbon Black によって自動的に保護させることができます。Daemonset は、通常、監視、ネットワーク、セキュリティ ソリューションに使用されます。このテクノロジーは、すべての Kubernetes で使用できます。
DevOps	従来の開発チームと IT 運用チームの統合。
Docker	オペレーティング システム レベルの仮想化（コンテナ）を提供するテクノロジー。Docker 環境には、コンテナ ランタイムとコンテナ ビルドとイメージ管理が含まれます。OCI 標準コンテナ イメージをビルドします。そのため、Docker イメージは OCI 準拠のコンテナ ランタイムで実行されます。
eBPF	カーネルのソース コードを変更したり、カーネル モジュールをロードしたりすることなく、カーネルの機能を安全かつ効率的に拡張するテクノロジー。
出力方向	クラスタから別のネットワーク（パブリックまたはプライベート）に送信されるトラフィック。
入力方向	クラスタの外部からクラスタ内のサービスに HTTP および HTTPS ルートを公開します。
Kubelet	ノードで実行されるエージェント。
Kubernetes	オープンソース コンテナ オーケストレータ。コンテナの展開、ロードバランシング、リソース割り当て、セキュリティの適用を自動化します。コンテナ化されたアプリケーションを目的の状態で稼動し続け、拡張性と耐障害性を確保します。
マニフェストのダイジェスト	SHA-256 で暗号化されたコンテナ イメージのハッシュで、イメージのビルドに基づいて確定されます。
マイクロサービス	独立し、緩やかに統合されたサービスのスイートに分割されたアプリケーション。
名前空間	単一クラスタ内のリソース グループを分離するためのメカニズム。
ノード	コンテナ化されたアプリケーションを実行するワーカー マシン。
ノード エージェント	すべてのノードがポッドのコピーを実行していることを確認します。ノード エージェントを使用すると、Kubernetes クラスタにノードを追加し、Carbon Black Container によって自動的に保護されるようにすることができます。
ポッド	実行中のコンテナのセット。
レジストリ	Docker Hub および他のサードパーティ リポジトリ ホスティング サービスはレジストリと呼ばれます。レジストリには、リポジトリのコレクションを保存します。
リポジトリ	特定のイメージの 1 つ以上のバージョンを保存します。
範囲	対象となるセキュリティ保護と分析のために Kubernetes リソースをグループ化する方法。たとえば、クラスタと名前空間ごとにリソースをグループ化し、その範囲のポリシーを作成できます。

用語	定義
テンプレート化されたポリシー	Carbon Black Cloud コンテナは、基本、限定的、および CIS ベンチマーク の 3 つのテンプレート化されたポリシーで展開します。
脆弱性スキャン	脆弱性スキャンは、既知の脆弱性を検出してセキュリティ侵害のリスクを軽減するのに役立ちます。コンテナ化されたアプリケーションの攻撃対象を減らします。
ワークロード	コンテナで実行されているアプリケーション。

ヒント: Kubernetes 用語の完全な用語集については、https://kubernetes.io/docs/reference/glossary/?fundamental=true を参照してください。

ランタイム ポリシーの概念と用語

ランタイム ポリシーには、Kubernetes 環境における出力方向ネットワーク制御、脅威からの保護、アノマリ検出のルールが含まれます。Kubernetes ワークロードの動作変更を制御するためのベンチマークを提供します。Kubernetes ランタイム環境の制御は、次の 2 つのレベルで実行されます。

- 範囲: 定義された範囲内のすべての Kubernetes リソースを監視できます。
- ワークロード: 特定のワークロードの動作を追跡できます。

アクション

すべてのルールには、関連付けられたアクション（監視 または アラート）があります。どちらのアクションでも、Carbon Black Cloud コンソールでアラートが発生します。

- [監視]: 監視アクションは、情報提供を目的としてイベント レコードを作成します。
- [アラート]: アラート アクションは、動作の変化を示すイベント レコードを作成します。アラートは、変更されない限り、各ルールのデフォルト アクションです。

組み込みルール

ランタイム ポリシーには、次のカテゴリの組み込みルールが含まれます。

- [出力方向トラフィック (範囲)] - 許可されたドメインまたは IP アドレスのリスト
- [悪意のある出力方向トラフィック (範囲)] — レピュテーションが悪い悪意のある IP アドレスとドメインのリスト
- [ワークロードのアノマリ検出] - ワークロードの動作の変化
- [ワークロードの脅威検出] - ポート スキャン

学習期間

学習期間は、範囲内のすべての Kubernetes リソースが出力方向ネットワーク接続を監視する時間です。出力方向の宛先はすべて、範囲ベースラインに記録されます。学習期間が完了したら、システムはワークロードの動作をアクティブに追跡します。後続の Kubernetes ランタイム ポリシーの違反はアラートをトリガします。

ポリシーの学習期間が変更されると、ポリシーはアラートを停止し、学習期間がリセットされます。新しいルールを追加すると、学習期間は新しいルールに対してのみ実行を開始します。

アアラートは、Carbon Black Cloud コンソールの Kubernetes アラートのトリアージ画面で確認および分析できます。

ルールの選択に使用する保護レベル

ランタイム ポリシー ルールは、以下の保護レベルに分けられます。

基本

優先順位が最も高い問題をカバーします。

中

[基本] 保護レベルに含まれるルールを拡張します。

厳密

[中] 保護レベルに含まれるルールを拡張します。最も広い範囲の問題を扱います。

ランタイム ポリシー範囲

Kubernetes 範囲は、クラスタやワークロードなどの Kubernetes リソースをグループ化したものです。Kubernetes ランタイム ポリシーでは、展開フェーズまたはターゲット完了アプリケーションを明示的に定義する範囲を使用します。

範囲ベースライン

範囲ベースラインは、範囲内のすべての Kubernetes リソースで許可される正常な動作を決定します。範囲ベースラインを確立するには、範囲内のすべてのワークロードの出力方向トラフィックを一定期間（学習期間 と呼ばれる）監視します。ベースラインからの逸脱はアラートをトリガします。ベースラインは範囲レベルにあり、範囲内の最終的な動作リストを修正またはリセットできます。

セキュリティ強化ポリシーの用語と概念

アクション

すべてのルールには、[アラート]、[ブロック]、[適用] に関連付けられるアクションがあります。ルール構成では、予期される値が設定されます。値が満たされない場合、ルール違反がトリガされます。

[アラート] アクション違反は、通知として表示されます。

[ブロック] アクションは、Kubernetes リソースをブロックします。この違反はアラートおよびブロック通知として表示されます。

[適用] アクションは、ルールの値を適用します。[適用] は、1 つ以上のフィールドの値を、ルールの事前設定で定義されている値に上書きします。つまり、[適用] は、設定をブロックするのではなく、変更します。たとえば、すべてのワークロードに CPU とメモリを設定できます。

注： 値を適用すると、実行中のワークロードは展開されたワークロードとは異なります。この違いはワークロードの動作に影響を与え、トラブルシューティングが必要な場合は混乱を引き起こす可能性があります。

組み込みルール

組み込みルールは、Kubernetes セキュリティ強化ポリシーで直接使用でき、Kubernetes セキュリティ構成に基づいています。

組み込みポリシーと範囲

Kubernetes ポリシーの初期設定を容易にするための、Carbon Black Cloud コンソールで使用可能なポリシーと範囲。これらのポリシーと範囲を更新および削除できます。詳細については、組み込みの Kubernetes セキュリティ強化ポリシーおよび組み込みの Kubernetes 範囲を参照してください。

コンテナ イメージの組み込みルール

コンテナ型のアイコン  を表示するルールは、CLI クライアントを使用してビルド フェーズの範囲に適用されます。ルールは、展開フェーズのコンテナ イメージに基づく Kubernetes ワークロードにも適用できます。これらのルールは、コンテナ イメージのプロパティと動作を強制します。このアイコンを表示しないルールは、ビルド フェーズには適用できません。組み込みの Kubernetes ポリシー ルールを参照してください。

カスタム ルール

カスタム ルールでは、JSONPath を使用して Kubernetes リソースとプロパティを指定します。

カスタム テンプレート

組み込みルールとカスタム ルールの組み合わせ。

例外

既知の動作と受け入れられた動作による Kubernetes ポリシーの対象からのワークロードの除外。

- ほとんどのルールで、例外はワークロード名に基づいています。
- ロールベースのアクセス制御 (RBAC) ルールの場合、例外はリソース名とユーザー名に基づきます。
- [適用] アクションを許可するルールの場合、例外はワークロード名またはワークロード ラベルに基づきます。

セキュリティ強化ポリシー

Kubernetes 環境構成のルールを確認するポリシー。

Kubernetes の範囲

ポリシーを適用するなどの明確な目的で Kubernetes リソースをグループ化します。

事前定義されたテンプレート

組み込みルールの事前定義されたルール セット。

違反

Kubernetes セキュリティ強化ポリシーを有効にした後に Kubernetes 環境で発生する変更に関する通知。違反は、ブロックまたはアラート ルール レベルでアクションをトリガします。ポリシーを有効にする前に潜在的な違反を特定できます。これにより、例外の追加、アクションの適用、ルールの無効化および有効化などのセキュリティ戦略の計画が可能になります。

コンテナ セキュリティ環境の設定

2

このセクションでは、Carbon Black Container を使用して Kubernetes を保護するための環境を整える方法について説明します。

次の基本的な手順に従って、Carbon Black Container セキュリティのためのコンテナ環境を設定します。

1 Kubernetes 環境が、Kubernetes Sensor のサポートされている動作環境要件を満たしていることを確認します。「Kubernetes センサー OER」を参照してください。

2 Kubernetes クラスタを Carbon Black Cloud コンソールに追加し、保護する各 Kubernetes クラスタに Kubernetes センサーをインストールします。

3 CLI クライアントをダウンロード、追加し、ローカル イメージをスキャンするように設定します。

これで、コンテナを管理するためのスコープとポリシーを作成する準備が整います。

次のトピックを参照してください。

- コンテナのロールとユーザー
- クラスタの追加と Kubernetes センサーのインストール
- Kubernetes センサーのステータスと健全性の確認
- イメージ スキャン用 CLI クライアントの設定

コンテナのロールとユーザー

コンテナでユーザーを追加し、作業に適切なロールを割り当てることができます。

ユーザーとそのロールを設定および管理することで、ユーザーは Carbon Black Cloud コンソールとコンテナ セキュリティ機能にアクセスできるようになります。

コンテナのロールの使用と作成

すべての Carbon Black Cloud コンソール ユーザーは権限を定義するロールに割り当てられます。ロールは、新しいユーザー アカウントを作成するときに割り当てられます。この割り当てはいつでも変更できます。

Carbon Black Cloud には、ユーザーに割り当てることができる（またはカスタム ロールを作成できる）4 つの Kubernetes 関連の事前定義ロールが含まれています（コンテナ ロールの追加を参照）。

- Kubernetes SecOps ビューのみ
- Kubernetes SecOps

- Kubernetes DevOps
- Kubernetes セキュリティ開発者

[Kubernetes Security DevOps] は、Kubernetes ワークロードの状態に対して責任があります。責任には、Kubernetes ワークロードのクラスタ、範囲、およびセキュリティ ポリシーの設定が含まれます。Security DevOps は、Kubernetes 環境の健全性を監視し、ワークロードと違反を調査して、適切なアクションを実行できます。

ロールの定義と推奨事項

次の表では、コンテナのユーザー ロールの Carbon Black Cloud 権限と推奨事項について説明します。

表 2-1. ユーザー ロール/権限マトリクス - ロール別

ロール	説明	権限	ワークフロー
[Kubernetes SecOps ビューのみ]	環境を監視します。アクションを実行できません。	■ 通知の表示 ■ Kubernetes セキュリティの表示 ■ イメージの表示 ■ ワークロードを表示	N/A
[Kubernetes SecOps]	ビルドからランタイムまで、ワークロードの攻撃対象を評価および制御します。コンテナ ランタイム スレッドの検出、応答、防止に重点を置いて、ランタイム スレッドをすばやく検出できます。 このロールは、SOC アナリストに適しています。	■ アラートの解除 ■ アラート、メモ、タグの表示および管理 ■ 通知の表示および管理 ■ API キーの表示および管理 ■ ユーザーの管理 ■ Kubernetes セキュリティの表示および管理 ■ イメージの表示 ■ イメージ例外の管理	1 コンテナを監視および分析します。を参照してください。 2 アクションを実行し、セキュリティの問題を修正します。「」「」「」を参照してください。 3 アラートをトリアージします。「」「」「」を参照してください。

表 2-1. ユーザー ロール/権限マトリクス - ロール別 （続き）

ロール	説明	権限	ワークフロー
[Kubernetes DevOps]	ビルドからランタイムまで、ワークロードの攻撃対象を評価および制御します。セキュリティの問題のトラブルシューティングと修正。 Kubernetes ワークロードの状態の判断に責任があります。責任には、Carbon Black Cloud コンソールの Kubernetes ポリシー、範囲、およびクラスタの設定が含まれます。Security DevOps は、Kubernetes 環境の健全性を監視し、ワークロードと違反を調査して、適切なアクションを実行できます。	■ アラートの解除 ■ 通知の表示および管理 ■ API キーの表示および管理 ■ ユーザーの管理 ■ Kubernetes セキュリティの表示および管理 ■ イメージの表示 ■ イメージ例外の管理	1 ユーザー ロールを設定し、ユーザーを管理します。コンテナのロールとユーザーを参照してください。 2 コンソールにクラスタを追加し、Kubernetes センサーをインストールします。クラスタの追加と Kubernetes センサーのインストールを参照してください。 3 コンテナを構成します。を参照してください。 4 コンテナを監視および分析します。を参照してください。 5 アラートをトリアージします。「」「」「」を参照してください。 6 アクションを実行し、セキュリティの問題を修正します。「」「」「」を参照してください。
[Kubernetes セキュリティ開発者]	単一のコンテナのセキュリティ状態とコンプライアンスを検査します。	■ Kubernetes セキュリティの表示および管理 ■ イメージの表示 ■ イメージ例外の管理	1 Kubernetes ワークロードを監視および分析します。を参照してください。 2 アラートをトリアージします。「」「」「」を参照してください。

コンテナ ロールの追加

コンテナの作業に新しいロールを追加するには、次の手順を実行します。

手順

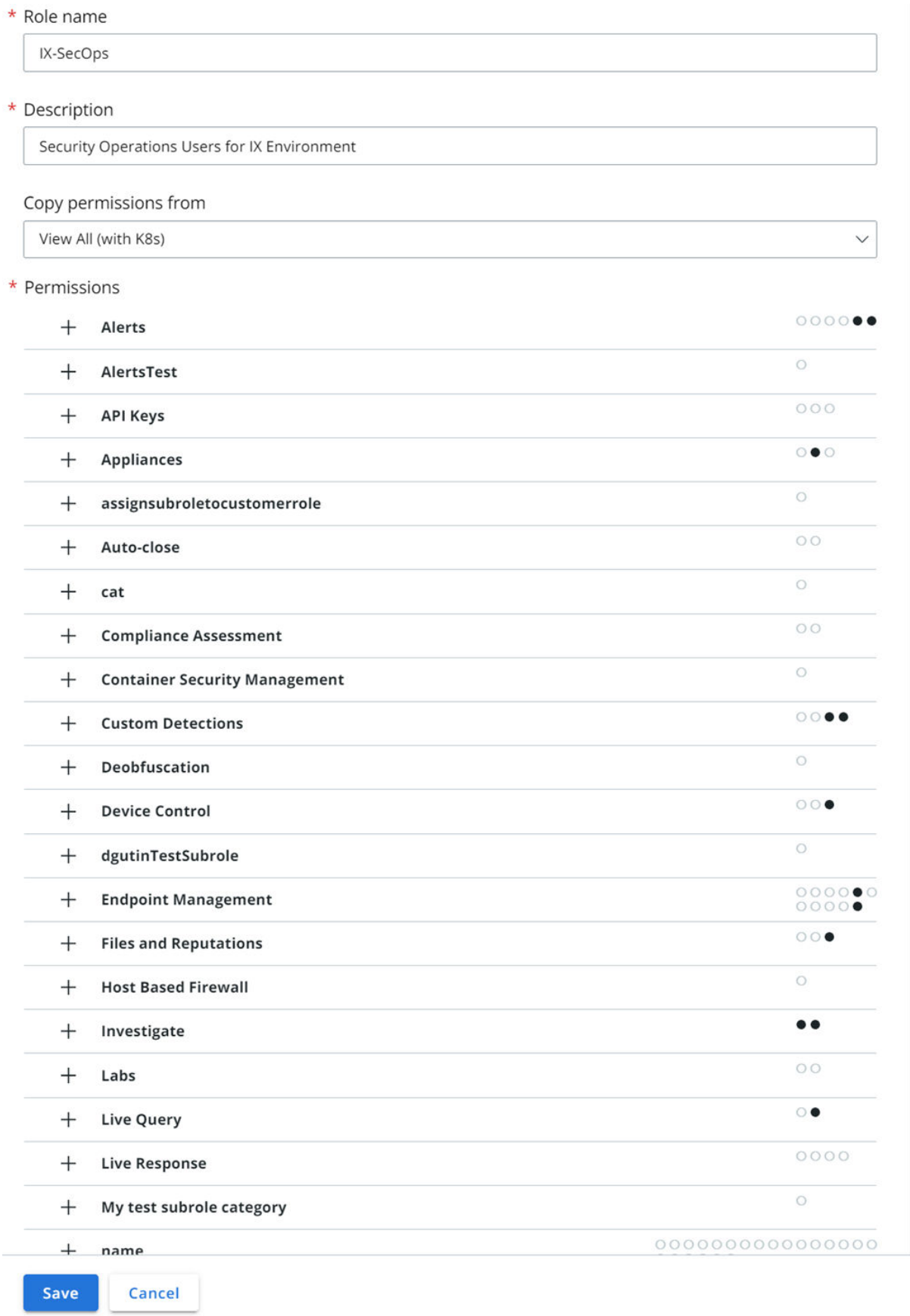
1 左側のナビゲーション ペインで、[設定] - [ロール] の順にクリックします。

2 画面の右上にある [ロールの追加] をクリックします。

3 新規ロールの一意の名前と説明を入力します。特殊文字は使用できません。

4 必要に応じて、[権限のコピー元] ドロップダウンからロールを選択し、既存のロールをテンプレートとして使用します。これにより、既存のロール権限のセットから、権限を追加および削除できます。

5 [権限] カテゴリを展開し、ロールの権限を選択または選択解除します。



コンテナ ロールの権限の詳細については、 コンテナのロールの使用と作成を参照してください。

6 [保存] をクリックします。

ヒント: ロールのコピーを作成するには、表のロールの横にある [複製]  アイコンをクリックします。コピーしたロールを使用して、新しいロールへの微調整が簡単にできます。

次のステップ

- 表内の新しいロールの右側にあるアイコンを使用して、ロールを複製、編集、エクスポート、または削除します。
- コンテナのためのユーザー アカウントの作成

コンテナのためのユーザー アカウントの作成

コンテナ作業用の新しいユーザー アカウントを作成するには、次の手順を実行します。

前提条件

コンテナのユーザーを作成する前に、使用可能なユーザー ロールを調査することをお勧めします。ユーザーには、割り当てられたロールに基づく権限が与えられます。事前定義済みのユーザー ロールを選択できます。既存のロールで環境に十分でない場合は、カスタム ロールを作成できます。コンテナのロールの使用と作成を参照してください。

手順

1 左側のナビゲーション ペインで、[設定] - [ユーザー] の順にクリックします。

2 画面の右上にある [ユーザーの追加] をクリックします。

3 名前、メール アドレス、ロールなどの新規ユーザーの詳細を入力します。

4 [保存] をクリックします。

結果

- メールが入力したメールアドレスに送信されます。ユーザーにログインしてパスワードを作成するよう求めるメールが送信されます。
- ユーザーがログイン認証情報を確認すると、追加されたユーザー名が表示されます。

クラスタの追加と Kubernetes センサーのインストール

Carbon Black Container を有効にするには、Kubernetes クラスタごとに 1 つの Carbon Black Kubernetes センサーをインストールする必要があります。そのためには、 コンソールにクラスタを追加する必要があります。

Kubernetes センサーの展開には、オペレータ と呼ばれる Kubernetes 拡張機能とオペレータ リソース定義が使用されます。オペレータは、ユーザー定義のコンポーネントを展開および管理し、その健全性を報告する一連のコントローラで構成されます。カスタム リソース定義を使用してコンポーネントを定義します。

Carbon Black オペレータは、クラスタ内に Kubernetes センサーを展開し、そのライフサイクルを管理します。カスタム リソース ファイルのデータは、センサーで有効にする機能を定義します。センサーの展開手順の基本的なステップは次のとおりです。

- Carbon Black オペレータのセットアップとインストール
- Carbon Black Cloud コンソールへのアクセスの許可
- Kubernetes センサーの構成

[クラスタの追加] ウィザードでは、次の手順を説明します。

クラスタの追加と Kubernetes センサーのインストール

Carbon Black Cloud コンソールにクラスタを追加し、そのクラスタに Kubernetes センサーをインストールするには、次の手順を実行します。

前提条件

開始する前に、Carbon Black Cloud コンソールとターミナル ウィンドウの両方を開きます。

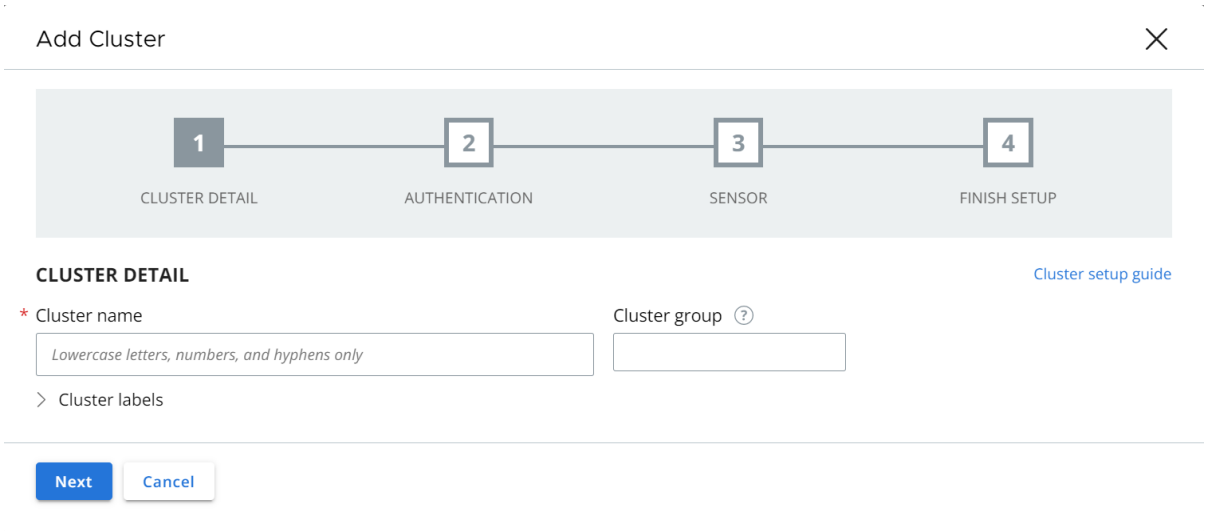
手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [クラスタ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [クラスタ] の順にクリックします。

2 画面の右上にある [クラスタの追加] をクリックします。

3 [クラスタの詳細] 情報を追加します。



a 小文字、数字、ハイフンを使用して、一意のクラスタ名を入力します。名前にコロン (:) 記号を含めることはできません。

b 既存のクラスタ グループを入力または選択して、範囲とポリシーにリソースを指定できるようにします。クラスタ グループは、クラスタのネットワーク アクティビティ マップの監視にも使用されます。

グループが指定されていない場合、クラスタは デフォルト グループに追加されます。

c 必要に応じて、クラスタ ラベルを追加します。ラベルは 1 つのキーと 1 つの値で構成されます。複数のラベルを追加できます。

4 [次へ] をクリックします。

5 Kubernetes クラスタと コンソール間の通信を確立するための専用 API キーを指定します。

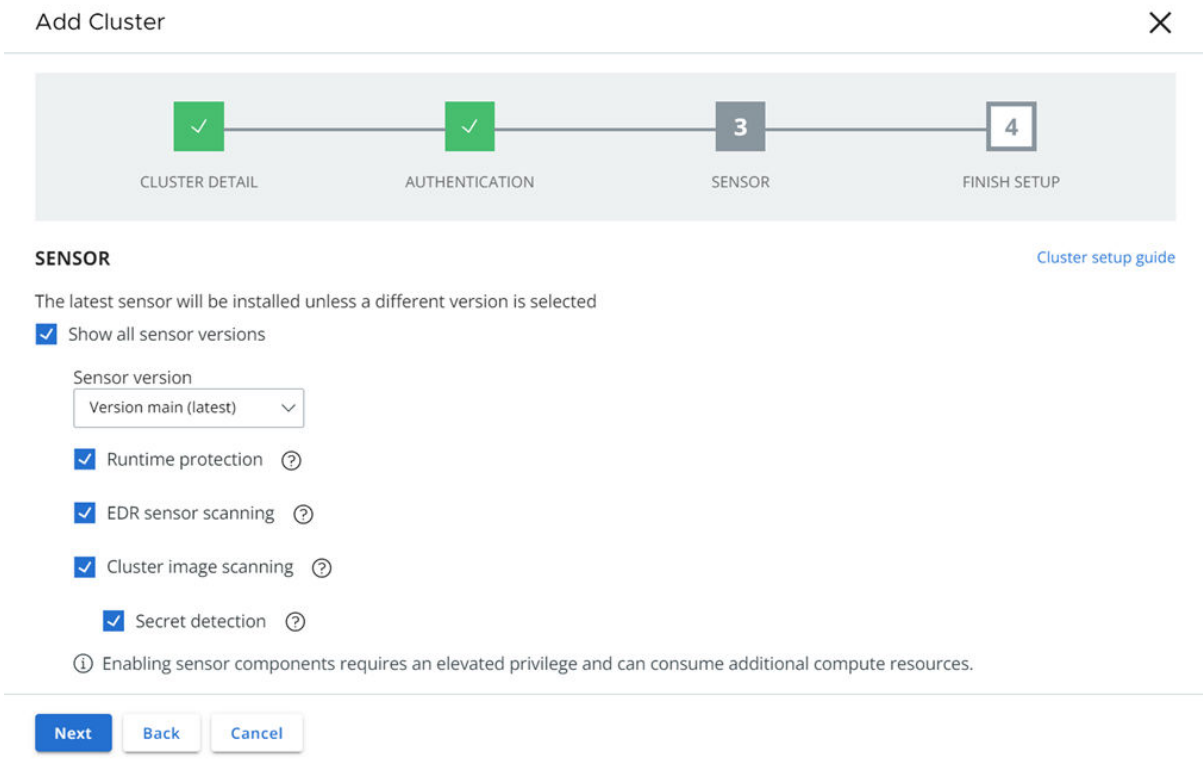
- [新しい API キーの生成] をクリックして、Carbon Black Cloud 組織に一意の API キー名を入力します。
- [既存の API キーを使用] をクリックして、既存の API キーを選択します。

重要： クラスタ間でキーを再利用しないでください。クラスタごとに個別の Carbon Black Cloud API キーを使用します。

6 クラスタにインストールする Kubernetes センサーのバージョンを選択します。デフォルトでは、最新のセンサー バージョンが設定されています。

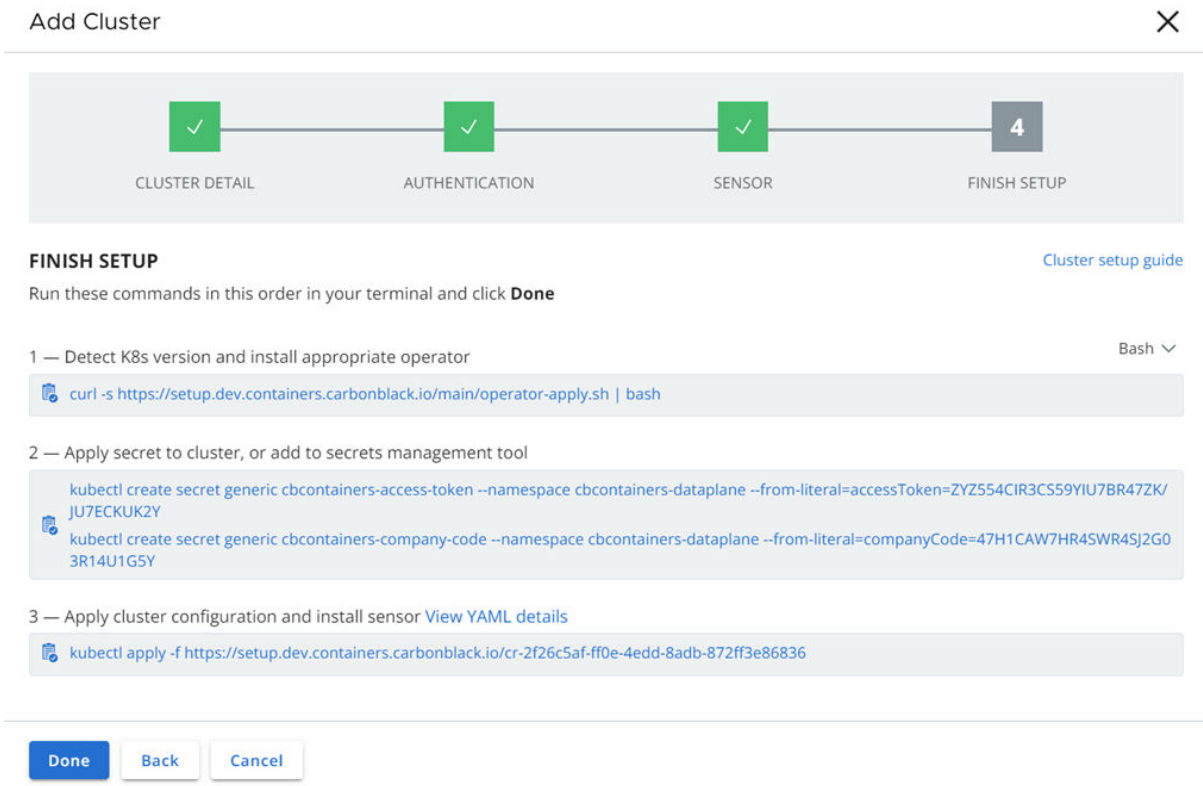
7 必要に応じて、次の設定を有効または無効にします。デフォルトでは有効になっています。Carbon Black では、これらの設定を有効にしてクラスタを完全に保護することをお勧めします。

- [ランタイム保護] — ポリシー ルールを使用して、展開されたワークロードの安全を確保できます
- [EDR センサー スキャン] — Kubernetes ノードからのアクティビティを監視して潜在的な脅威を特定します
- [クラスタ イメージのスキャン] — クラスタ イメージの最初のスキャンと自動再スキャンが有効になります
- [シークレット検出] — コンテナ イメージ内のシークレットのスキャンを有効にします



8 [セットアップの終了] 画面で、右上のドロップダウン メニューから [Bash] または [PowerShell] を選択します。

9 各コマンドを順番にターミナルにコピーして実行します。



10 コンソールで、[完了] をクリックします。

11 コンソールのブラウザ画面を更新して、新しいクラスタを表示します。

クラスタのステータスは [インストール保留中] になります。

初期セットアップ中にクラスタが安定するまでに最大 5 分かかります。その間、ステータスがエラーとして表示される場合があります。インストール リクエストの送信後、3 ～ 5 分間待ってから正しいステータスを確認してください。

結果

セットアップ手順が正常に完了すると、ステータスが [実行中] に変わります。

次のステップ

1 CLI クライアントのダウンロード

2 CLI クライアントの追加と構成

3 Kubernetes センサーのステータスと健全性の確認

Kubernetes センサーのステータスと健全性の確認

クラスタ内の Kubernetes センサーのステータスを表示するには、次の手順を実行します。

手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [クラスタ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [クラスタ] の順にクリックします。

2 [Kubernetes クラスタ] 画面で、[クラスタ] タブをクリックし、[全般] タブをクリックします。

3 左側のペインで、表示されるクラスタのリストを次の方法でフィルタリングできます。

- ステータス
- センサーのバージョン
- オペレータ バージョン
- クラスタ ラベル キー
- クラスタ ラベル値

4 [クラスタ] パネルでは、クラスタを検索できます。また、表示されたクラスタ名を選択して、センサーの健全性データを表示できます。

5 クラスタを選択し、右側のパネルに [ステータス] を表示します。

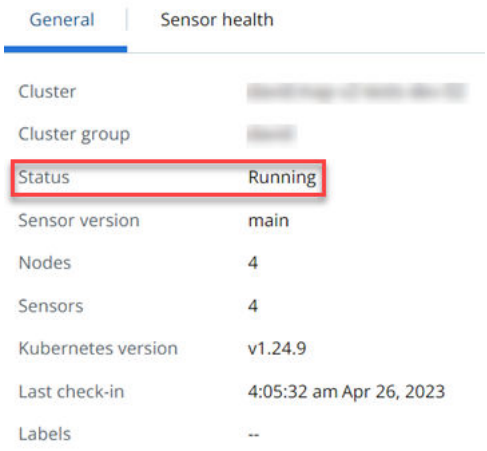


表 2-2. Kubernetes センサーのステータス

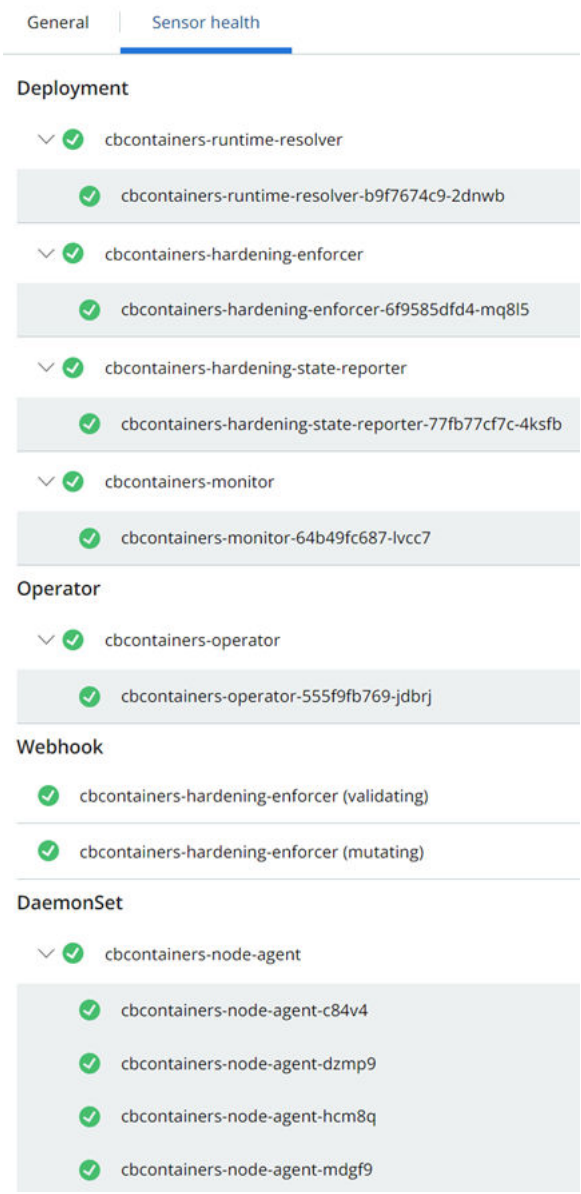
ステータス	説明
クリティカル	どのクラスタ コンポーネントからも 24 時間以上アクティビティが検出されていません
エラー	重要度の高いコンポーネントがダウンしているか、ステータスを検出できません
保留中のインストール	クラスタのセットアップが進行中です

表 2-2. Kubernetes センサーのステータス （続き）

ステータス	説明
実行中	すべてのコンポーネントがエラーなしで稼動しています
警告	重要度の低いコンポーネントがダウンしているか、ステータスを検出できません

6 [センサーの健全性] タブをクリックします。

エントリを展開するには、左側の矢印  アイコンをクリックします。例：



イメージ スキャン用 CLI クライアントの設定

イメージ スキャンを継続的に統合スクリプトに含めるには、Carbon Black Cloud CLI クライアント (`Cbctl`) を構成して使用します。このクライアントは、Linux および macOS で使用できます。

CLI クライアントは Dev/Sec/Ops マシンにインストールしたり、Jenkins や Gitlab などの CI/CD パイプラインに含めたりすることができます。CLI クライアントには、Carbon Black Cloud へのインターネット接続とコンテナ レジストリへのアクセスが必要です。

Carbon Black CLI クライアントは、既知の脆弱性のイメージ スキャンを実行し、セキュリティ ルールまたはコンプライアンス ルールを適用します。CLI クライアントは次のタスクを実行します。

- ［コンテナ イメージの脆弱性スキャン］。

コンテナ イメージは、既知の脆弱性データベースと照合されます。イメージの詳細には、オペレーティング システムとオペレーティング システム以外のパッケージ、ライブラリ、ライセンス、バイナリ、メタデータが含まれます。脆弱性スキャンの結果は、イメージ メタデータに含まれています。

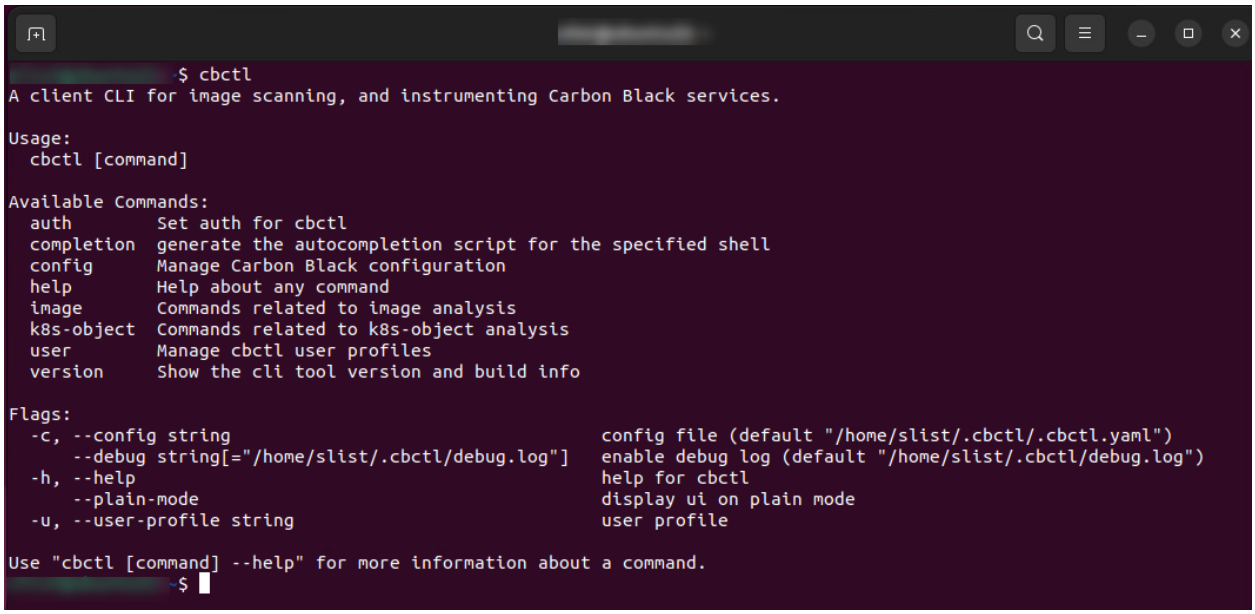
- [コンテナ イメージの基準を強化]。

  ポリシー違反を評価するため、イメージ スキャンの結果は、CLI 範囲用に構成された特定のポリシーと照合されます。ポリシー違反が検出された場合、CLI の実行でビルド パイプラインの手順に失敗します。ポリシー ルールの違反は、イメージ ルールの例外とともにイメージ メタデータに追加されます。

- [Kubernetes ワークロードの基準を強化]。

  セキュリティ リスクのワークロード コンプライアンスを評価するため、Kubernetes ワークロードは Kubernetes セキュリティ強化ポリシーと照合されます。イメージの脆弱性とワークロードの構成の両方の情報を活用することで、ワークロードのリスク エクスポージャの全体像を把握できます。

CLI クライアントには、次のインターフェイスとコマンド オプションが表示されます。



シークレット ファイルの検出

シークレット検出が有効になっている場合、Carbon Black Cloud はイメージ内のすべてのテキスト ファイルを検出します。ファイルは無視できます。これらは、CLI フラグを使用して指定されます。スキャン時間を短縮するため、システム ファイルはデフォルトで無視されます。

注： シークレット検出を有効または無効にするには、「クラスタの追加と Kubernetes センサーのインストール」を参照してください。

表 2-3. CLI フラグ

フラグ	説明	デフォルト設定
enableSecretDetection	シークレットをスキャンするかどうかを示す	False
skipDirsOrFiles	シークレットをスキャンしないファイルまたはディレクトリ	N/A
scanBaseLayers	基本レイヤのシークレットをスキャンするかどうかを示す	False
ignoreBuildInRegex	スキャンでファイルの組み込み正規表現を無視するかどうかを示す	False

CLI クライアントのダウンロード

構成した CLI インスタンスを追加して、イメージのローカル スキャン、ワークロードの脆弱性評価、および CI インテグレーションを有効にします。CLI インスタンスはコンテナ イメージをスキャンし、その健全性を Carbon Black Cloud コンソールに報告します。

手順

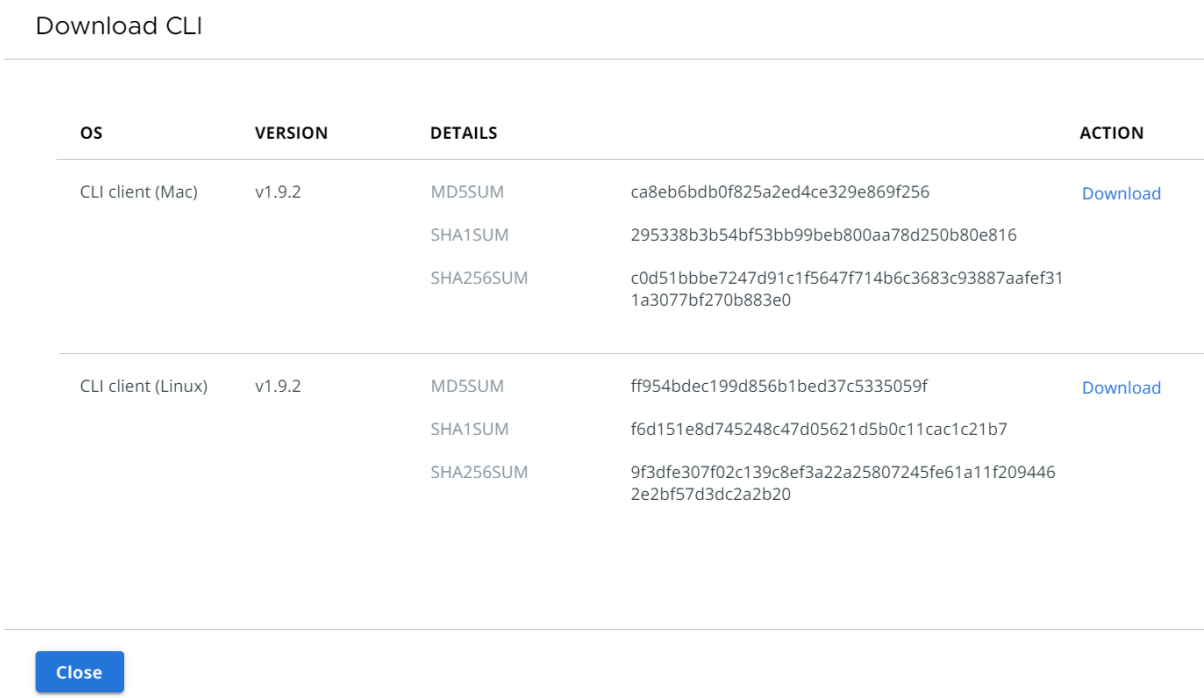
1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [クラスタ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [クラスタ] の順にクリックします。

2 [CLI の構成] タブをクリックします。

3 画面の右上にある [CLI のダウンロード] をクリックします。

4 オペレーティング システム（macOS または Linux）の CLI クライアントを選択してダウンロードします。



5 [閉じる] をクリックします。

次のステップ

CLI クライアントの追加と構成

CLI クライアントの追加と構成

イメージ スキャン用の CLI インスタンスを設定するには、次の手順を実行します。

構成した CLI インスタンスを追加して、イメージのローカル スキャン、ワークロードの脆弱性評価、および CI インテグレーションを有効にします。CLI インスタンスはコンテナ イメージをスキャンし、その健全性を Carbon Black Cloud コンソールに報告します。

前提条件

CLI クライアントのダウンロード

開始する前に、Carbon Black Cloud コンソールとターミナル ウィンドウの両方を開きます。

手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [クラスタ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [クラスタ] の順にクリックします。

2 [CLI の構成] タブをクリックします。

3 画面の右上にある [CLI の追加] をクリックします。

a この CLI インスタンスの一意の名前を入力します（API キー名とは異なります）。

小文字、数字、ハイフンのみを使用します。この名前は、コンソールで CLI を識別および管理するのに役立ちます。

b CLI 実行のデフォルト フィールドとして使用するビルド手順の名前（開発、本番、コンプライアンスなど）を入力します。

ビルド ステップは、ビルド フェーズ範囲で参照 ID として使用され、関連する構成済み CLI との接続を確立します。ビルド手順のパラメータは、Carbon Black Cloud の範囲を照合し、その範囲のポリシーを引き続き適用するために使用されます。デフォルトの範囲は構成ファイルに保存されます。

注：

- デフォルトのビルド手順は固有ではありません。複数の CLI インスタンスが、同じデフォルトの範囲を使用できます。[デフォルトのビルド手順]は、構成ファイルを直接編集しない限り、初期設定後に変更することはできません。
- ビルド手順のパラメータなしでスキャンが呼び出された場合、構成ファイルのデフォルトのビルド手順が使用されます。
- [ビルド手順] で、[Kubernetes] > [範囲] 画面のこの値を使用するビルド フェーズの範囲を作成します。を参照してください。
- CLI `validate` コマンドを使用する必要があります。

c オプションの説明を追加します（推奨）。

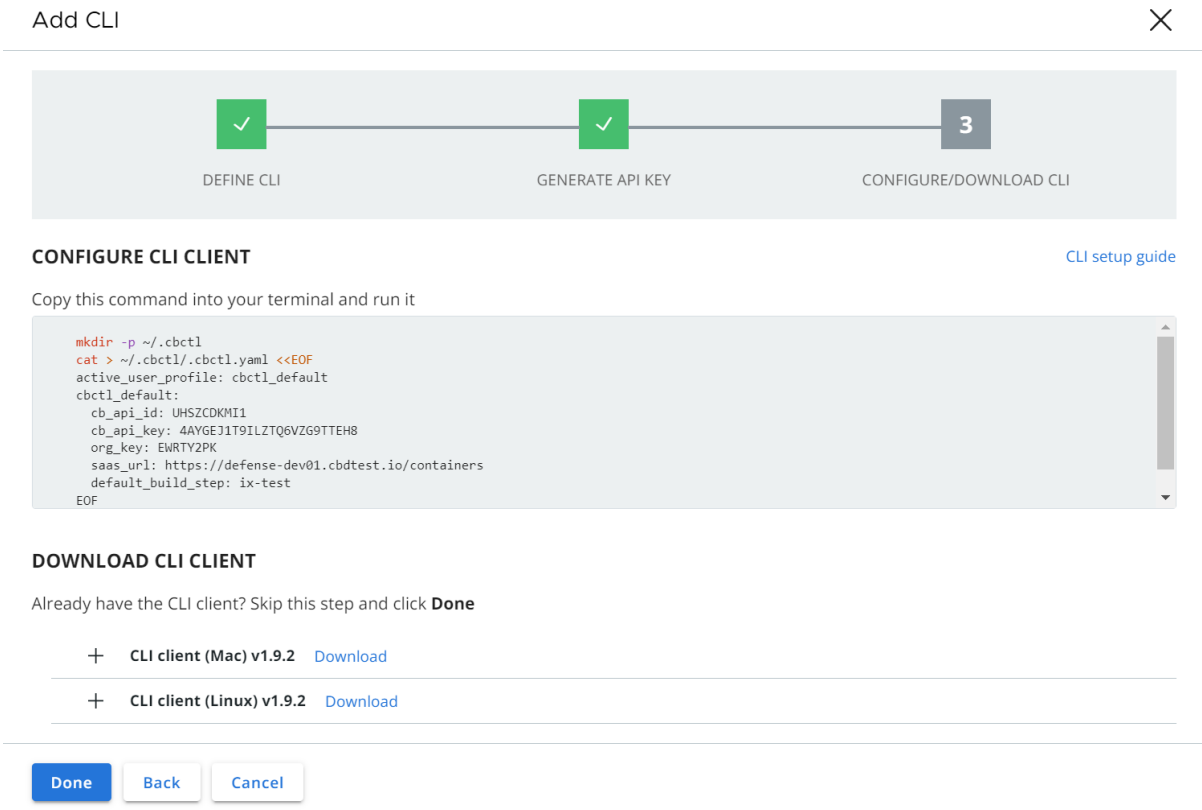
4 [次へ] をクリックします。

5 一意の API キー名を入力し、[生成] をクリックします。

6 [次へ] をクリックします。

7 ターミナル ウィンドウで次のコマンドをコピーして実行します。

```
mkdir -p ~/.cbctl
cat > ~/.cbctl/.cbctl.yaml <<EOF
active_user_profile: cbctl_default
cbctl_default:
  cb_api_id: UHSZCDKMI1
  cb_api_key: 4AYGEJ1T9ILZTQ6VZG9TTEH8
  org_key: EWRTY2PK
  saas_url: https://defense-dev01.cbdtest.io/containers
  default_build_step: ix-test
EOF
```



8 CLI クライアントをまだダウンロードしていない場合は、CLI インスタンス バイナリ ファイルを今すぐ選択してダウンロードし、ビルド環境で実行できます。

9 [完了] をクリックします。

結果

ターミナルで構成された CLI クライアントを操作して、コンテナ イメージの脆弱性スキャンの結果を確認できます。

次のステップ

イメージ スキャン CLI API を実行するには、Container Security API および統合を参照してください。

Kubernetes に展開されたコンテナ イメージの脆弱性スキャンを監視するには、[インベントリ] - [Kubernetes] - [コンテナ イメージ] 画面に移動します。

特定のリポジトリにあるがまだ展開されていないコンテナ イメージのイメージ スキャン結果を表示するには、[インベントリ] - [Kubernetes] - [コンテナ イメージ] 画面に移動し、[イメージ リポジトリ] タブをクリックします。

コンテナ セキュリティの構成

3

このセクションでは、コンテナ セキュリティの構成に関連するタスクについて説明します。

次のトピックを参照してください。

- Kubernetes 範囲
- 出力グループ
- Kubernetes ポリシー
- アラート通知のサブスクライブ
- API アクセスの設定

Kubernetes 範囲

Kubernetes 範囲は目的を共有する Kubernetes リソースのグループです。たとえば、クラスタは Kubernetes リソースであり、範囲定義の対象となります。範囲をフィルタとして使用することも、Kubernetes リソース全体に同じセキュリティ ポリシーを適用することもできます。

Kubernetes リソースを範囲でグループ化することで、セキュリティ ポリシーの対象となる計画を立てることができます。範囲を追加および編集したり、Kubernetes ポリシーに関連付けられていない範囲を削除したりできます。

デフォルトの範囲

デフォルトの範囲とは、すべてのクラスタと名前空間を含む事前定義された範囲です。デフォルトの範囲は 任意 と呼ばれます。任意の範囲は常に使用可能で、削除できません。これは、スコープの階層内で最も高い範囲です。範囲解決プロセスは、ポリシーを適用するために Kubernetes リソースが分類される最も正確な範囲定義を検索します。より正確な範囲が見つからない場合は、デフォルトの範囲に添付されているポリシーが考慮されます。

ビルド フェーズの範囲

ビルド フェーズ とは、CLI クライアント コマンドを使用してスキャンまたは検証するためのコンテナ イメージまたは Kubernetes オブジェクトを定義することを指します。コマンドは CI/CD パイプラインに統合できます。ビルド フェーズ内のすべてのリソース、Kubernetes 名前空間、または特定のビルド手順の範囲を定義できます。ビルド手順は、CLI クライアントがイメージ スキャンの実行に使用するパラメータです。イメージ スキャン用 CLI クライアントの設定および 4 章 イメージのスキャンを参照してください。

展開フェーズの範囲

展開フェーズ とは、展開されるまたはすでに展開されている Kubernetes ワークロードのグループ化を指します。

範囲は、すべてのクラスタ、クラスタ グループ、クラスタ、名前空間、ワークロード の順序に従って、最も一般的なものから最も具体的なものまで、階層によって重複する可能性があります。重複範囲の一部であるワークロードの場合、最も狭い範囲に関連付けられるポリシーが適用されます。これにより、ワークロードは 1 つのポリシーに解決されます。

Kubernetes 範囲階層を参照してください。

例： 例

範囲の例	目的
すべての本番クラスタのクラスタ グループ	同じ階層のすべてのクラスタに対してポリシーをフィルタリングするまたは割り当てるため。
1 つ以上の Kubernetes クラスタ	ポリシーをフィルテリングする、または別のクラスタに割り当てるため。
複数のクラスタに定義された Kubernetes 名前空間の選択によるクラスタ間のアプリケーション	ポリシーをフィルタリングする、または展開されている場所に関係なく、アプリケーションを形成するリソースのグループに割り当てるため。

アプリケーション範囲

アプリケーション範囲 にはビルド フェーズと展開フェーズの両方のコンテナ イメージが含まれます。範囲は、アプリケーションを独自の Kubernetes 名前空間に分離する方法を反映しています。範囲がアプリケーション範囲として定義される場合、範囲に割り当てられたポリシーは、開発フェーズに関係なく、また、この名前空間が格納されているクラスタに関係なく、名前空間内のすべてのコンテナ イメージに適用されます。この範囲により、アプリケーションのビルドまたは展開時に同じセキュリティ強化基準が確保されます。

Kubernetes 範囲階層

Kubernetes 範囲階層は、範囲解決プロセスにとって重要です。範囲解決プロセスは、ワークロードが存在する最も具体的な範囲を見つけ、その範囲で Kubernetes ワークロードに適用するポリシーを定義します。

重複範囲の Kubernetes ワークロードの範囲解決

範囲は設計によって重複しています。つまり、ワークロードは複数の重複する範囲に属している可能性があります。ただし、Kubernetes ワークロードはそれぞれ 1 つの ポリシー に関連付けられます。範囲の解決ロジックを実行することで、システムは各ワークロードの最も具体的な範囲に関連するポリシーを見つけます。

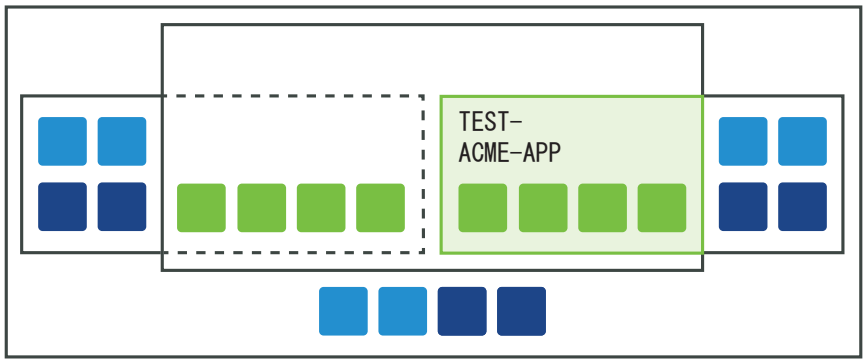
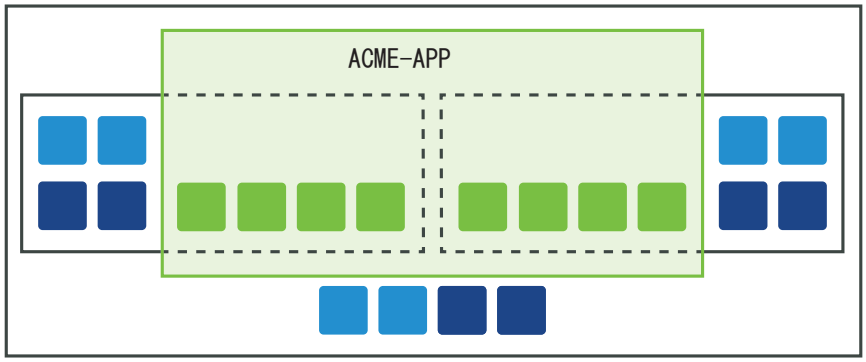
範囲を計画することで、他のシステムに影響を与えることなく、Kubernetes 環境内の特定の領域に適用されるポリシーを決定できます。

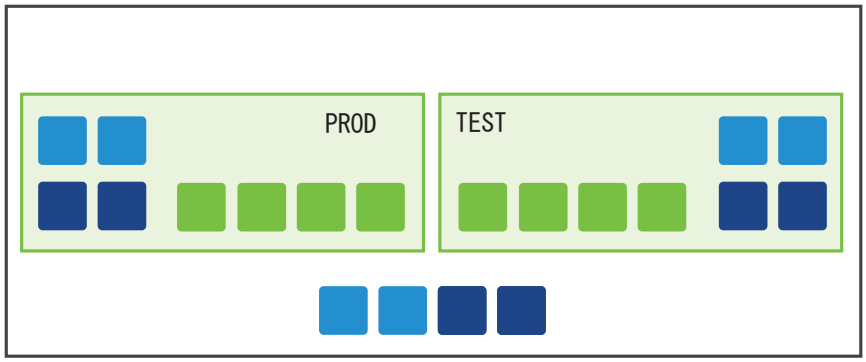
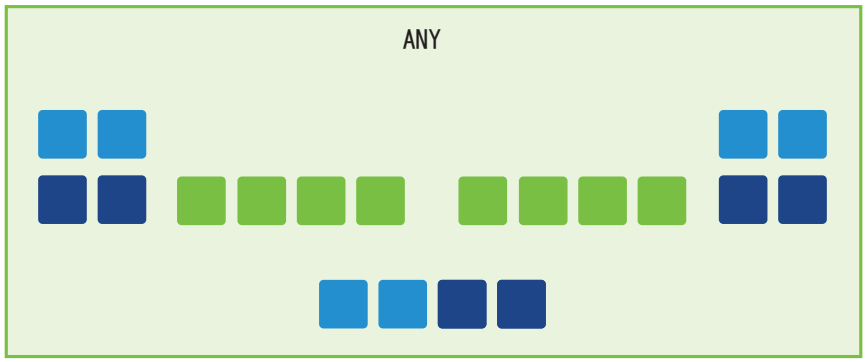
範囲のランク付け

範囲は、特性別にランク付けされます。具体的な範囲は、一般的な範囲よりも優先されます。

次の図は、範囲をランク付けしています。図には、クラスタ グループと名前空間内のワークロードのさまざまな色のボックスと、それらを含む範囲の緑色のボックスが表示されます。最も具体的な範囲は階層の一番上にあります。

例： 範囲の例図

ランク付け	説明
特定のクラスタ内の特定の名前空間内のリソース。	特定の Kubernetes セキュリティ強化ポリシーを使用するための範囲の最も具体的な定義。
特定のクラスタ グループ内の特定の名前空間内のリソース	クラスタ グループ内のこれらの特定の名前空間のみがカバーされます。
特定のクラスタ内のリソース	クラスタ内のすべての名前空間がカバーされます。隔離されたテスト クラスタでアプリケーションをテストする範囲の例: test-acme-app 
任意のクラスタ内の特定の名前空間内のリソース	名前空間に対して定義され、名前空間を含むすべてのクラスタに対して有効なアプリケーション範囲。名前空間をカバーする Kubernetes 環境全体の範囲の例: acme-app 

ランク付け	説明
特定のクラスタ グループ内のリソース	この高レベルな範囲は、クラスタのグループをカバーします。本番環境とテスト環境の 2 つの範囲の例: 
すべてのリソース - [任意] の範囲を参照してください。	デフォルトの[任意]の範囲には、システム内のすべてのワークロードが含まれ、他のすべての範囲と重複しています。特定の Kubernetes リソースの範囲は、デフォルトの範囲よりも優先されます。 

組み込みの Kubernetes 範囲

Kubernetes クラスタをインストールして設定すると、システムにはすぐに使用できる 3 つの範囲 ([Kubernetes システム]、[CBContainers データプレーン]、[デフォルトの名前空間]) が含まれます。

組み込み範囲は組み込みのセキュリティ強化ポリシーに割り当てられます。範囲は設定の開始点として使用でき、編集または削除できます。組み込みのセキュリティ強化ポリシーの構成の詳細については、組み込みの Kubernetes セキュリティ強化ポリシーを参照してください。

事前にパッケージ化された範囲	範囲ターゲット	範囲の説明
Kubernetes システム	[ターゲット:] 展開フェーズ [名前空間:] kube-system	Kubernetes システムによって作成されたオブジェクトの名前空間と一致します。通常、このシステムには DNS、プロキシ、コントローラ マネージャ、およびその他のシステム コンポーネントのサービスが含まれます。
CBContainers データプレーン	[ターゲット:] 展開フェーズ [名前空間:] cbcontainers-dataplane octarine-dataplane	Carbon Black Kubernetes エージェントが実行され、そのリソースを展開する名前空間と一致します。 **注：** 2 つの名前空間がここに表示されます。Octarine-dataplane は、エージェントのバージョン 3.0.0 より前の名前空間名です。Cbcontainers-dataplane は現在の名前空間名です。
デフォルトの名前空間	[ターゲット:] 展開フェーズ [名前空間:] デフォルト	名前空間が指定されていないオブジェクトを保持する Kubernetes 組み込みデフォルト名前空間と一致します。

注： 組み込み範囲が変更されていない場合、[最終変更者] パラメータは [Carbon Black] です。範囲を編集すると、[最終変更者] パラメータも変更されます。

Kubernetes リソースへの Kubernetes アプリケーション範囲の追加

Kubernetes リソースは範囲でグループ化できます。範囲のターゲットは アプリケーション です。

前提条件

Kubernetes クラスタを設定します。クラスタの追加と Kubernetes センサーのインストールを参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [範囲] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [範囲] の順にクリックします。

2 [範囲の追加] をクリックします。

3 範囲の[名前]を入力します。

4 ターゲット リソースの場合は、[アプリケーション] を選択します。この範囲は、特定の名前空間内のアプリケーションをターゲットにします。ポリシーは、ビルド、展開、実行の各フェーズ中に適用できます。

5 [次へ] をクリックします。

6 ドロップダウン メニューから名前空間を選択します。

7 [保存] をクリックします。

範囲は、Kubernetes セキュリティ強化ポリシーで使用する準備ができています。

次のステップ

Kubernetes セキュリティ強化ポリシーの作成

Kubernetes リソースへの Kubernetes 展開場所の範囲の追加

Kubernetes リソースは範囲でグループ化できます。範囲ターゲットは 展開場所

前提条件

Kubernetes クラスタを設定します。クラスタの追加と Kubernetes センサーのインストールを参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [範囲] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [範囲] の順にクリックします。

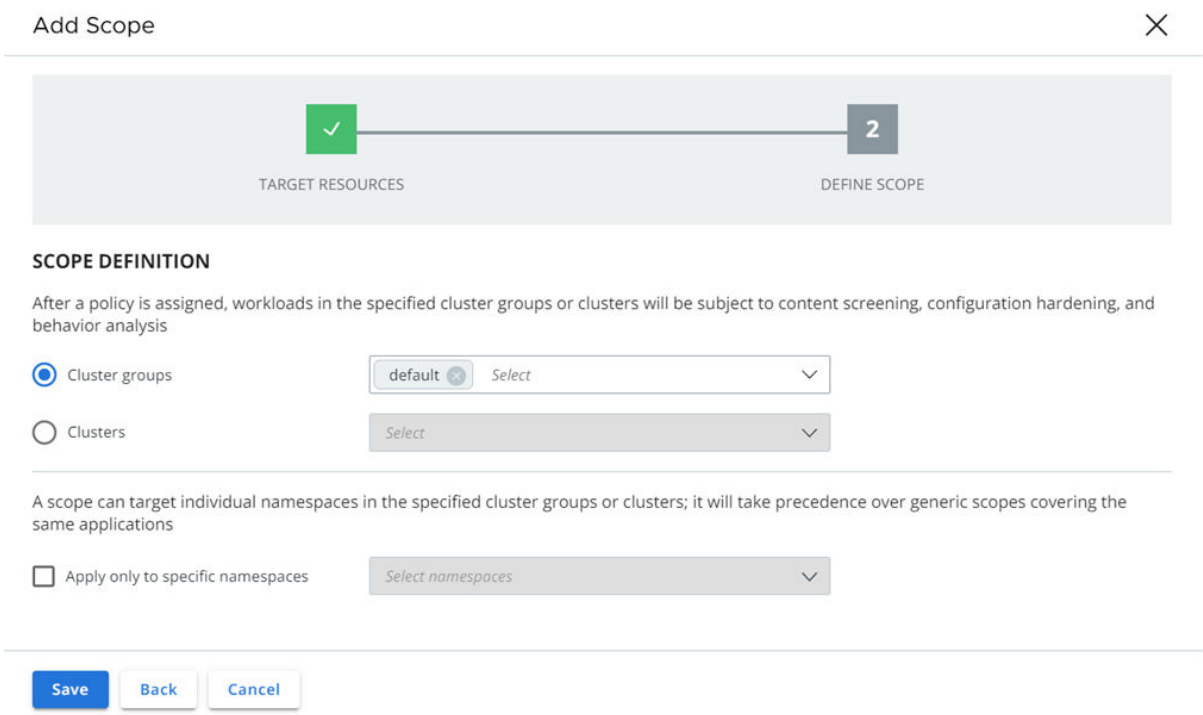
2 [範囲の追加] をクリックします。

3 範囲の[名前]を入力します。

4 ターゲット リソースの場合は、[展開場所] を選択します。この範囲は、特定のクラスタまたはクラスタ グループ内のワークロードを対象にします。ポリシーは、展開フェーズと実行フェーズ中に適用できます。

5 [次へ] をクリックします。

6 範囲のターゲットを選択します。



- クラスタ、名前空間、またはその両方でグループ化できます。
- 同一のポリシーを複数のクラスタに適用するには、範囲の基準としてクラスタ グループを使用します。クラスタ グループの代わりに個々のクラスタを選択することもできます。クラスタ グループには、既存または将来のすべてのクラスタが含まれます。したがって、クラスタ グループは、クラスタのリストを選択するよりも幅広い選択肢になります。
- 複数のクラスタに同じ名前の名前空間がある場合、名前空間ごとに定義する範囲は、その名前空間のクラスタ間に及びます。
- 特定のクラスタ内の特定の名前空間を決定するには、クラスタまたはクラスタ グループと特定の名前空間を提示できます。

7 [保存] をクリックします。

範囲は、Kubernetes セキュリティ強化ポリシーで使用する準備ができています。

次のステップ

Kubernetes セキュリティ強化ポリシーの作成

Kubernetes リソースへの Kubernetes コンテナ イメージ範囲の追加

範囲を使用して、まだ展開されていないコンテナ イメージにポリシーを適用できます。範囲の対象はビルド フェーズです。

前提条件

Kubernetes クラスタを設定します。クラスタの追加と Kubernetes センサーのインストールを参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [範囲] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [範囲] の順にクリックします。

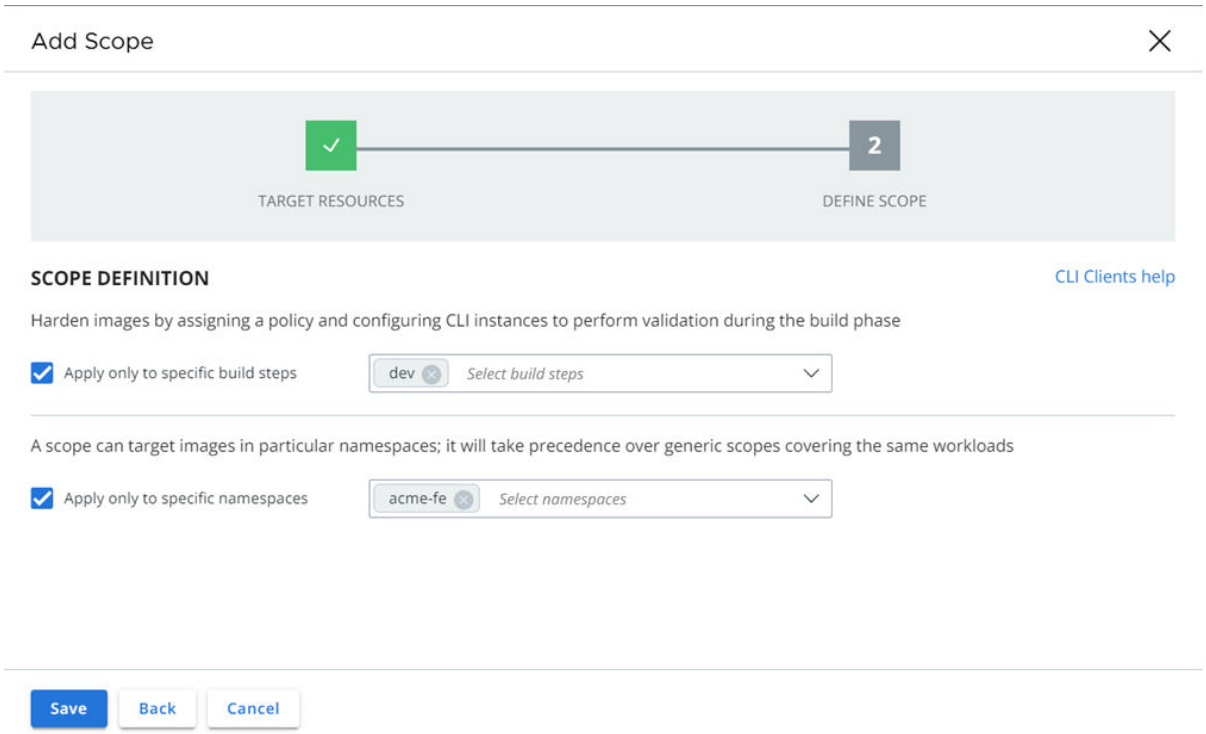
2 [範囲の追加] をクリックします。

3 範囲の[名前]を入力します。

4 ターゲット リソースの場合は、[コンテナ イメージ] を選択します。この範囲は、特定のコンテナ イメージを対象とします。ポリシーは、ビルド フェーズ中に適用できます。

5 [次へ] をクリックします。

6 ドロップダウン メニューからターゲット基準を選択します。



オプション	説明
[特定のビルド手順にのみ適用]	ビルド フェーズ中に検証を実行するようにポリシーを割り当て、CLI インスタンスを構成してイメージを強化します
[特定の名前空間にのみ適用]	範囲は、特定の名前空間のイメージをターゲットにすることができます。同じワークロードをカバーする一般的な範囲よりも優先されます

7 [保存] をクリックします。

範囲は、Kubernetes セキュリティ強化ポリシーで使用する準備ができています。

次のステップ

Kubernetes セキュリティ強化ポリシーの作成

Kubernetes 範囲の表示

Kubernetes 範囲を表示するには、次の手順を実行します。

手順

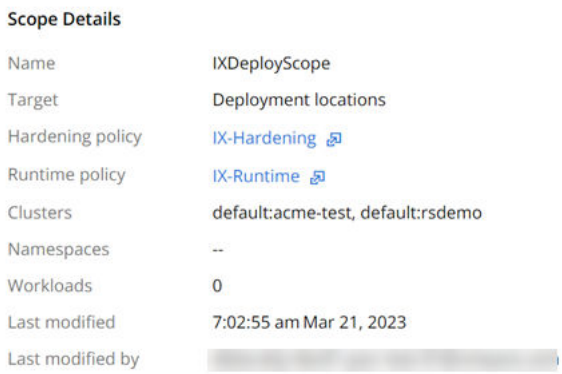
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [範囲] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [範囲] の順にクリックします。

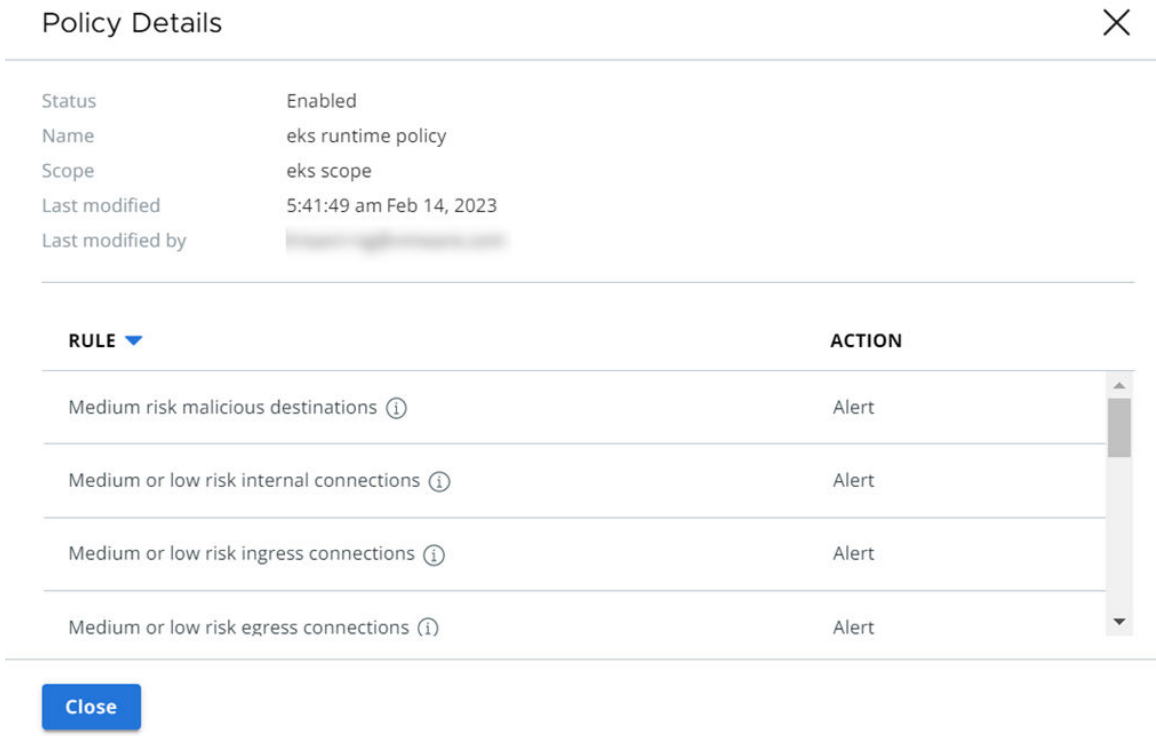
左側のペインには、範囲、添付されたポリシー、および各範囲の影響を受けるワークロードの数が表示されます。

2 左側のペインで、範囲を選択します。

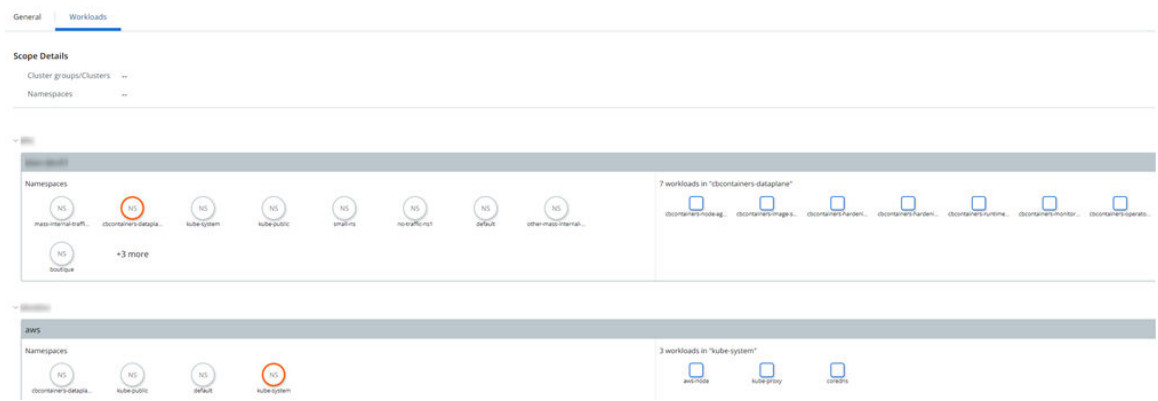
- [全般] タブをクリックして、範囲の詳細を表示します。



- 範囲にポリシーが添付されている場合は、ポリシー名をクリックしてそのポリシーのサマリを表示できます。例：



- また、この範囲でカバーされる名前空間とワークロードを表示することもできます。[ワークロード] タブをクリックして、名前空間を表示します。その名前空間内のワークロードを表示するには、名前空間をクリックします。



Kubernetes 範囲の編集または削除

Kubernetes 範囲の構成を更新できます。範囲名と含まれるリソースのみを更新できます。範囲ターゲットは更新できません。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [範囲] の順にクリックします。

- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [範囲] の順にクリックします。

2 左側のペインで、範囲を選択します。[全般] タブで、[オプション] ドロップダウン メニューから [編集] をクリックします。

ヒント: 範囲を削除するには、[削除] をクリックし、[OK] をクリックして削除を確定します。

3 [次へ] をクリックします。

4 名前または含まれているリソースを変更し、 [保存] をクリックします。

ランタイム ポリシーの Kubernetes 範囲ベースライン

Kubernetes 範囲ベースラインはランタイム ポリシーに適用されます。ベースラインの動作は、学習期間中に検出された範囲でグループ化されたすべてのワークロードの通常のアクティビティを反映します。学習期間は、範囲内のすべての Kubernetes リソースが出力方向ネットワーク接続を監視する時間です。出力方向の宛先はすべて、範囲ベースラインに記録されます。

範囲ベースラインは、範囲内のすべての Kubernetes リソースで許可される正常な動作を決定します。ベースラインからの逸脱はアラートをトリガします。ベースラインは範囲レベルにあり、最終的な動作リストを修正またはリセットできます。

ランタイム ポリシーの Kubernetes 範囲ベースラインの表示

ランタイム ポリシーの Kubernetes 範囲ベースラインを表示するには、次の手順を実行します。

手順

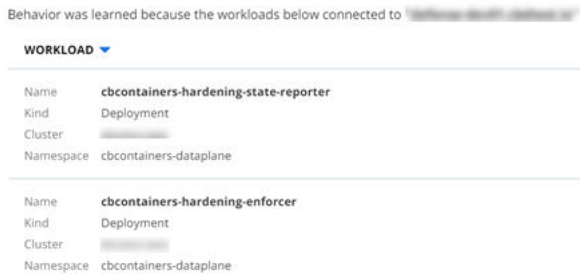
1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 ポリシーを選択し、行の最後にある矢印  をクリックして [ポリシーの詳細] パネルを開きます。

4 [ポリシーの詳細] パネルで、[範囲ベースラインの表示] をクリックします。

ベースラインの動作が左側のペインに表示されます。ベースラインから動作を削除したり、動作を選択して右側のペインに追加情報を表示したりできます。例：



次のステップ

範囲ベースラインに動作を追加したり、範囲ベースラインをリセットしたりできます。

Kubernetes 範囲ベースラインへの動作の追加

学習期間をリセットしたり、ベースラインから何も削除することなく、学習期間の完了後に Kubernetes ランタイム ポリシーの範囲ベースラインを変更できます。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 ポリシーを選択し、行の最後にあるキャレット  をクリックして [ポリシーの詳細] パネルを開きます。

4 [ポリシーの詳細] パネルで、[範囲ベースラインの表示] をクリックします。

5 [動作を追加] をクリックします。

6 宛先のタイプを選択します。パブリック ドメインまたはプライベート ドメイン、サブドメイン、または IP アドレス範囲を入力して、[追加] をクリックします。

結果

出力方向トラフィックの宛先が範囲ベースラインに正常に追加されました。

誤検出を通常動作として範囲ベースラインに追加

アラートの Kubernetes ランタイム ポリシーの範囲ベースラインを調整できます。これは、ワークロードの動作の誤検出を示します。これを行うには、アラートを閉じるか、出力方向トラフィックの宛先を範囲ベースラインに追加します。

一般的に、Kubernetes ランタイム ポリシーの有効化、または更新後、学習期間の完了後にアラートを確認します。問題を解決するか、アラートを閉じることで、アラートの数を減らせます。

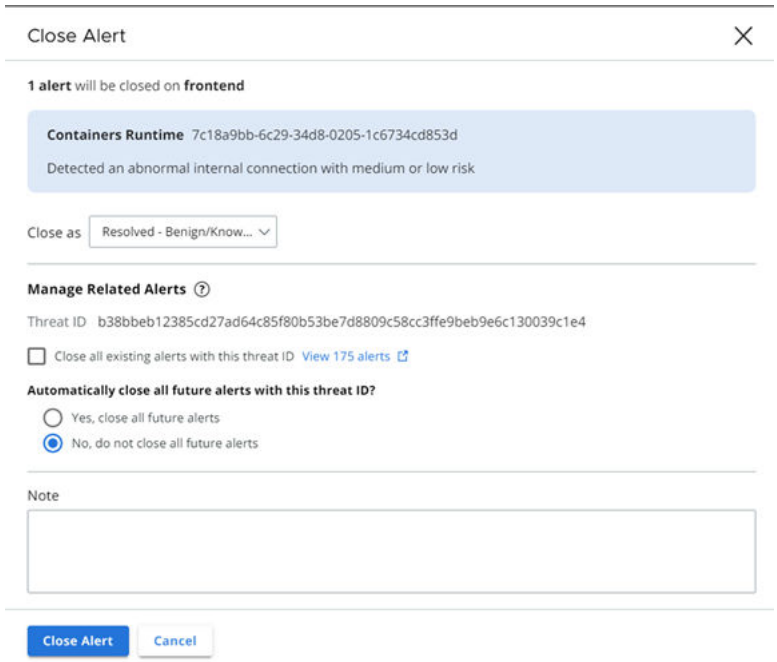
注： アラートを閉じることは、既知の動作を示す特定のワークロードをアラート リストから除外する場合にのみ推奨されます。

手順

1 左側のナビゲーション ペインで、[アラート] を選択します。

2 関心のあるアラートを見つけて選択し、次のいずれかを実行します。

- [アクション] ドロップダウン メニューで [ベースラインに追加] をクリックします。[OK] をクリックして確認します。
- [アクション] ドロップダウン メニューで [閉じる] をクリックします。



a [閉じる理由] ドロップダウン メニューで、アラートを閉じる理由を選択します（例: [解決済み - 無害/既知]）。

b 必要に応じて、このチェック ボックスを選択して、同じ脅威 ID を持つ既存のすべてのアラートを閉じます。

c 必要に応じて、この脅威 ID を持つ今後のすべてのアラートを自動的に閉じます。

d アラートを閉じる理由に関するオプションのメモを入力します。

e [アラートを閉じる] をクリックします。

Kubernetes 範囲ベースラインのリセット

Kubernetes 範囲ベースラインをリセットするには、次の手順を実行します。

ベースラインのリセットは、イメージが変更され、新しい動作が以前に学習した動作と異なる場合に重要です。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 範囲に関連付けられているポリシーを見つけて、行の最後にある矢印  アイコンをクリックします。

4 [リセット] をクリックします。

結果

範囲ベースラインとポリシー学習期間がリセットされます。

出力グループ

出力グループは、ネットワーク マップ上のクラスタからの出力方向トラフィックのプレゼンテーションを編成します。ドメインと IP アドレスに基づいて、クラスタの出力グループを定義します。

デフォルトの出力グループには、パブリックとプライベートの 2 つのグループがあります。パブリック出力には、ネットワークの外部に送信されるトラフィックが含まれます。プライベート出力は、IP アドレスのプライベート アドレス空間を使用する出力方向トラフィックで構成されます。

注： 宛先が 2 つ以上の出力グループに分類される場合、トラフィックは最も具体的な出力グループの下に表示されます。

出力グループの作成

出力グループを定義するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ネットワーク] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ネットワーク] の順にクリックします。

2 [出力グループ] タブをクリックし、[グループの追加] をクリックします。

3 グループの [名前] と [説明] を入力します。

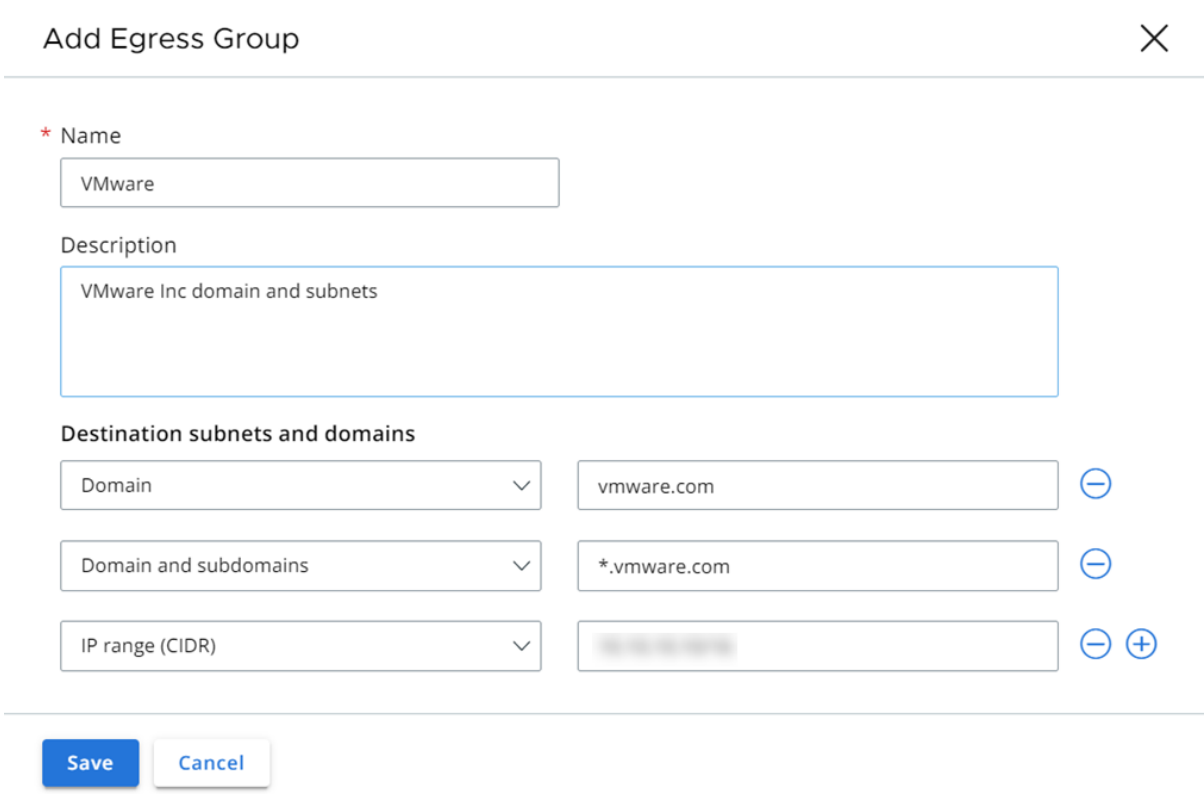
4 グループの[宛先サブネットとドメイン]を定義します。論理 AND 演算子を使用して、宛先を一連のルールとして構成します。構成可能なオプションは次のとおりです。

a [DNS ドメイン名] - ドメイン名と完全に一致

b [DNS ドメイン名とサブドメイン] - サブドメインのサフィックスを含むすべてのドメイン名

c [IP アドレス範囲] — サブネット マスクまたは IPv6 表記を使用するクラスレス ドメイン間ルーティング (CIDR)

例：



5 [保存] をクリックします。

出力グループの編集または削除

出力グループを編集または削除するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ネットワーク] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ネットワーク] の順にクリックします。

2 [出力グループ] タブをクリックします。

3 編集または削除する出力グループを選択します。

- 出力グループを編集するには、[編集]  アイコンをクリックします。グループ構成を更新し、[保存] をクリックします。
- 出力グループを削除するには、ゴミ箱アイコン をクリックし、[削除] をクリックして確認します。

Kubernetes ポリシー

Carbon Black Cloud の Kubernetes ポリシーは、Kubernetes 環境のセキュリティ強化に役立つように、セキュリティ ルールをポリシーにグループ化します。

Carbon Black Container Kubernetes ポリシーは、保護する環境のタイプ（ランタイム または セキュリティ強化）によって定義されます。各 Kubernetes ポリシーは特定の Kubernetes 範囲にバインドされ、各範囲は 1 つのポリシーに割り当てられます。ランタイム ポリシーとセキュリティ強化ポリシーは、共通の範囲を共有できます。これにより、ポリシー違反の根本原因を追跡できます。

注： タイプを指定せずに Kubernetes ポリシーが参照されている場合、両方のタイプのポリシーが参照されます。

Kubernetes ランタイム ポリシー

Kubernetes ランタイム ポリシーは、出力方向トラフィック、脅威、およびアノマリに関連する Kubernetes 環境の動作と変更を監視するルールのグループです。Kubernetes ランタイム ポリシーは、Kubernetes ワークロードの実行中に許可される動作を定義します。

ランタイム ポリシーの概念と用語を参照してください。

Kubernetes ランタイム ポリシーの作成

Kubernetes ランタイム ポリシーを作成するには、次の手順を実行します。

前提条件

すべての前提条件はオプションです。

- ランタイム ポリシーの概念と用語を参照します。
- Kubernetes ランタイム ポリシーにリンクする Kubernetes 範囲を作成します。Kubernetes 範囲を作成するには、Kubernetes 範囲を参照してください。範囲を事前に作成していない場合は、Kubernetes ランタイム ポリシーを作成するときに作成できます。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 [ポリシーの追加] をクリックします。

4 [ポリシーの定義] 画面でポリシーに名前を付け、使用可能な範囲のリストから範囲を選択して、[次へ] をクリックします。

注： このポリシーで使用する範囲を構成していない場合は、[範囲の追加] をクリックします。詳細な手順については、Kubernetes リソースへの Kubernetes アプリケーション範囲の追加を参照してください。

5 [ルールの追加] 画面で、ポリシーに含めるルールを選択します。

ルールは、[基本]、[中]、および [厳密] テンプレートから追加できます。これらのテンプレートの詳細については、Kubernetes ポリシー テンプレートを参照してください。

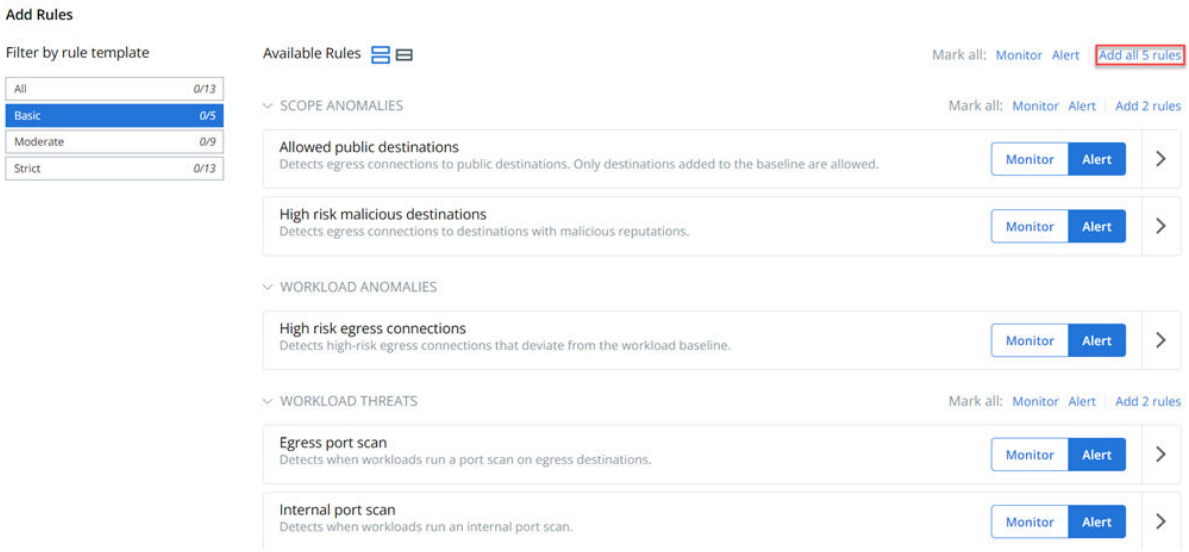
重要： Carbon Black では、重要度が最も高い問題のアラートを提供する [基本] テンプレートのルールから始めることをお勧めします。

たとえば、[基本] テンプレートからすべてのルールを追加するには、次の手順を実行します。

a 左側の [基本] ルール テンプレートを選択します。

b 右上にあるアラート アクションのタイプ ([監視] または [アラート]) を選択します。[アラート] がデフォルトのアクションです。

c 右上の [5 つのルールをすべて追加] をクリックします。



ルールを一括で追加する代わりに、テンプレートから個別のルールを追加できます。そのためには、ルールの右側にある矢印  アイコンをクリックします。

ルールを追加すると、画面の右側のペインにルールが表示されます。ここから、個別のルールまたはすべてのルールを削除できます。

注： 独自のテンプレートを作成できます。Kubernetes ポリシー テンプレートの作成を参照してください。

6 [次へ] をクリックします。

7 ポリシー設定を確認します。範囲ベースラインの学習期間を設定します。デフォルト値は 7 日です。学習期間中の範囲ベースラインの進行状況を確認するには、ランタイム ポリシーの Kubernetes 範囲ベースラインの表示を参照してください。

- [ポリシーを有効にする] をクリックしてポリシーを作成し、有効にします。
- [ドラフトとして保存] をクリックして、ポリシーをドラフト状態で保存します。この場合、Carbon Black Cloud はポリシーを [無効] として保存します。ポリシーを編集して有効にできます。Kubernetes ランタイム ポリシーの編集および Kubernetes ランタイム ポリシー ドラフトを有効にするを参照してください。

次のステップ

Kubernetes ランタイム ポリシーを構成し、学習期間が終了すると、動作ベースラインが確立され、保護がアクティブになります。ランタイム ポリシーの違反によって発生したすべてのアラートは、[アラート] 画面に表示されます。Kubernetes アラートのトリアージを参照してください。

Kubernetes ランタイム ポリシーの編集

Kubernetes ランタイム ポリシーを編集するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 編集するポリシーを選択し、 [アクション] ドロップダウン メニューで [ポリシーの編集] をクリックします。

注： ランタイム ポリシーのフィールドとルールの詳細については、Kubernetes ランタイム ポリシーおよび Kubernetes ランタイム ポリシーの作成を参照してください。

a ポリシーがリンクされている範囲を変更し、[次へ] をクリックします。

b 必要に応じてルールを追加または削除し、[次へ] をクリックします。

c 必要に応じて学習期間を調整し、[保存] をクリックします。

Kubernetes ランタイム ポリシー ドラフトを有効にする

[無効] になっている Kubernetes ポリシーを有効にできます。[無効] 状態のポリシーは、作成時にドラフトとして保存されました。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ランタイム ポリシー] タブをクリックします。

3 [無効] ステータスのポリシーを選択し、[アクション] ドロップダウン メニューで [ポリシーを有効にする] をクリックします。

結果

ポリシーがすぐに有効になります。

Kubernetes ランタイム ポリシーの詳細の表示

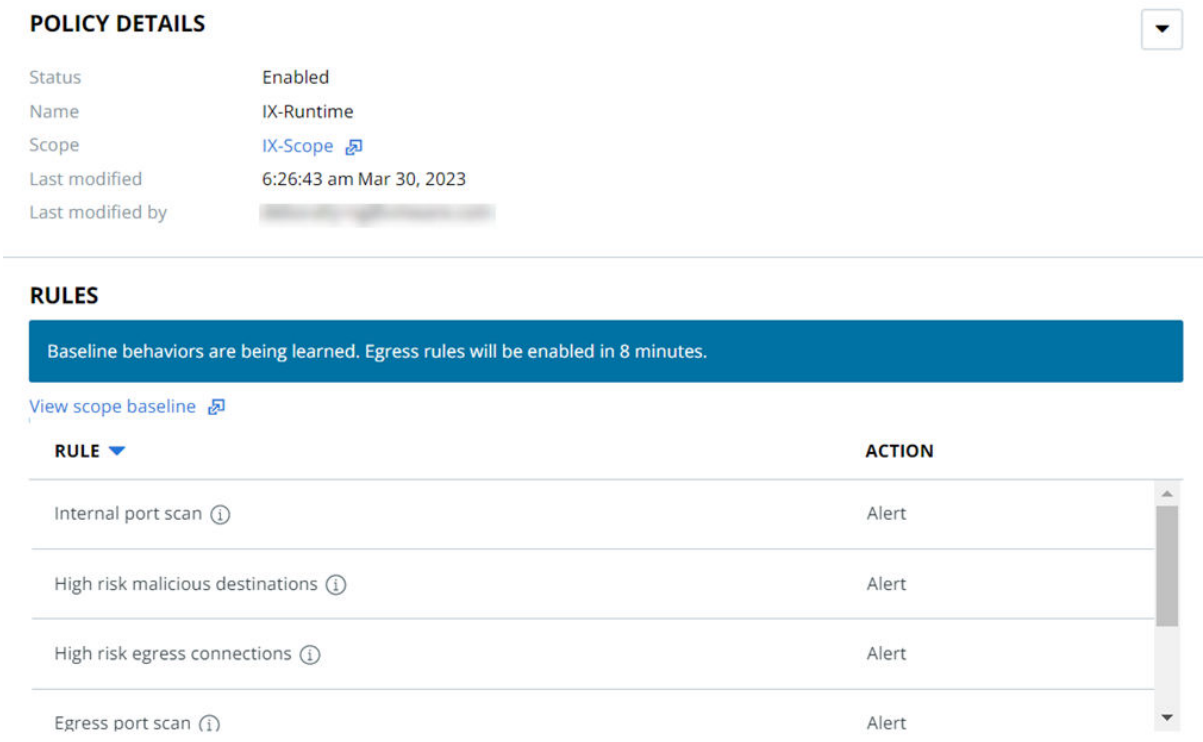
Kubernetes ランタイム ポリシーの詳細を表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

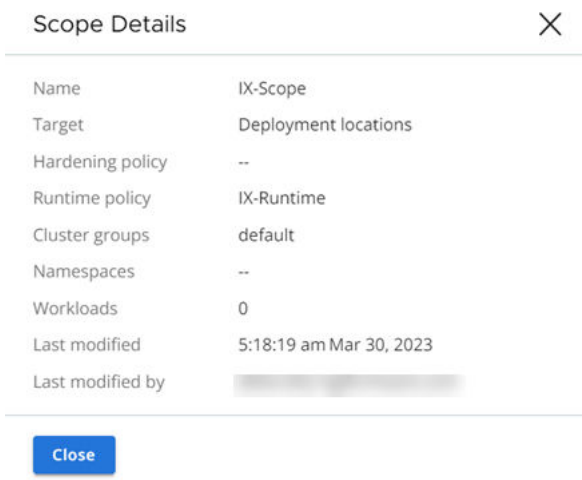
2 [ランタイム ポリシー] タブをクリックします。

3 表示するポリシーを選択し、ルールの右側にある矢印  アイコンをクリックします。



4 次の詳細を表示できます。

- [ステータス]、[名前]、[範囲]、[最終変更日]、[最終変更者] データ。追加の範囲の詳細を表示するには、[範囲] 名をクリックします。



- ルールのステータス（学習モードの場合）
- ルールとそのアクション
- 範囲ベースライン。[範囲ベースライン表示] をクリックして、ベースラインを表示および管理します。ランタイム ポリシーの Kubernetes 範囲ベースラインを参照してください。

Kubernetes セキュリティ強化ポリシー

Kubernetes セキュリティ強化ポリシーは、Kubernetes リソースのターゲット構成を説明する事前定義済みポリシー ルールとユーザー定義ポリシー ルールの組み合わます。Kubernetes セキュリティ強化ポリシーは、ワークロード構成のセキュリティを確保します。

セキュリティ強化ポリシーの用語と概念を参照してください。

組み込みの Kubernetes セキュリティ強化ポリシー

Kubernetes クラスタをインストールして設定すると、システムにはすぐに使用できる 2 つポリシー ([Kube システム] と [CBContainers データプレーン]) が含まれます。

組み込みポリシーは組み込み範囲に関連付けられます。組み込み範囲の詳細については、組み込みの Kubernetes 範囲を参照してください。

ポリシーは設定の開始点として使用でき、編集または削除できます。

ヒント: ポリシーを複製したり、複製を変更したりできるため、参照用の元のポリシーを維持できます。

組み込みポリシー	割り当てられた範囲
Kube システム	Kubernetes システム
CBContainers データプレーン	CBContainers データプレーン

組み込みポリシーが変更されていない限り、[最終変更者] パラメータは [Carbon Black] です。ポリシーを編集すると、[最終変更者] パラメータも変更されます。

組み込みポリシーには、すべての Kubernetes セキュリティ強化ポリシーで使用できる組み込みルールのサブセットが含まれています。

Kubernetes セキュリティ強化ポリシーの作成

Kubernetes ワークロードとコンテナ イメージにルールを適用する Kubernetes セキュリティ強化ポリシーを作成できます。

前提条件

すべての前提条件はオプションです。

- セキュリティ強化ポリシーの用語と概念を参照します。
- Kubernetes セキュリティ強化ポリシーにリンクする Kubernetes 範囲を作成します。Kubernetes リソースへの Kubernetes アプリケーション範囲の追加を参照してください。範囲を事前に作成していない場合は、Kubernetes セキュリティ強化ポリシーを作成するときに作成できます。
- Kubernetes セキュリティ強化ポリシーでカスタム ルールを使用するには、セキュリティ強化ポリシーを作成する前にカスタム ルールを作成する必要があります。Kubernetes セキュリティ強化ポリシーのカスタム ルールを参照してください。
- 新しいポリシーに適用するカスタム ルール テンプレートを作成します。Kubernetes ポリシー テンプレートの作成を参照してください。
- ルールに [適用] アクションを適用するには、適用事前設定を追加する必要があります。適用する事前設定を参照してください。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 [ポリシーの追加] をクリックします。

4 [ポリシーを定義] 画面で、次の手順を実行します。

   a ポリシーに名前を付けます。

   b 使用可能な範囲のリストから範囲を選択するか、[範囲の追加] をクリックして、このポリシーで使用する新しい範囲を構成します。Kubernetes リソースへの Kubernetes アプリケーション範囲の追加を参照してください。

   c 初期コンテナを有効にするには、[初期コンテナを含める] テキスト ボックスを選択します。

   初期コンテナは、Kubernetes ポッドのアプリケーション コンテナの前に実行される特殊なコンテナです。初期コンテナには、アプリケーション イメージには存在しないユーティリティまたはセットアップ スクリプトを含めることができます。初期コンテナには、多くの場合、より多くの権限がありますが、有効期限が短いためクラスタの全体的なセキュリティに与える影響は少なくなります。

d　一時コンテナはデフォルトで選択されています。

一時コンテナは、ポッド内のデバッグに役立つ特別なタイプのコンテナです。このポリシーに関連付けられた一時コンテナを使用しない場合は、[一時コンテナを含める] チェック ボックスの選択を解除します。一時コンテナの詳細については、一時コンテナを参照してください。

e　[次へ] をクリックします。

5　[ルールの追加] 画面で、ポリシーに含めるルールを選択します。

- カテゴリ内のすべてのルールまたはテンプレートのすべてのルールを追加できます。デフォルトですべてのルールに [アラート] アクションが設定されます。アクションを [ブロック] または [適用] にリセットできます。

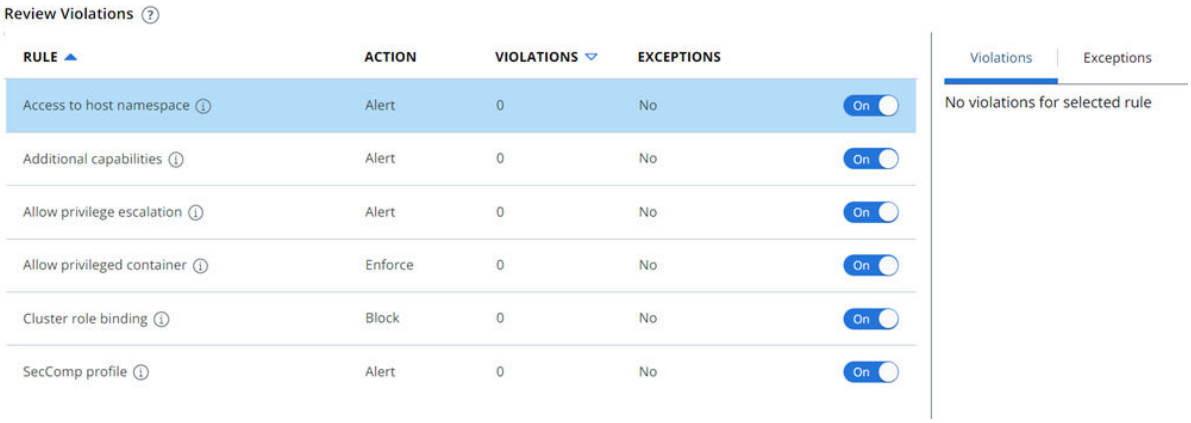
  重要：

  - 適用ルールは、`kube-system` 名前空間では動作しません。この名前空間では、重要なシステム リソースへの予期しない変更を防止するためのブロック ルールとして機能します。
  - 必要に応じて、[適用] アクションの定義済み事前設定を含めるか、適用事前設定を追加します。ルールでユーザー入力が必要な場合は、[適用事前設定] ドロップダウン メニューが表示されます。適用する事前設定を参照してください。

- ルールを一括で追加する代わりに、テンプレートから個別のルールを追加できます。そのためには、ルールの右側にある矢印  アイコンをクリックします。
- ルールを追加すると、画面の右側のペインにルールが表示されます。ここから、個別のルールまたはすべてのルールを削除できます。

6　[次へ] をクリックします。

7 [違反の確認] 画面で、ポリシーを有効にした後に通知が送信される違反の可能性を確認します。



注： 例外を作成できます。[例外] タブをクリックしてから、[条件の追加] をクリックします。Kubernetes セキュリティ強化ポリシー ルールの例外の作成を参照してください。

8 ルールの `On` と `Off` を切り替えて、セキュリティ強化ポリシーで現在アクティブなルールを定義します。

9 [次へ] をクリックします。

10 [ポリシーの確認] 画面で、[ポリシーを有効にする] をクリックします。

- [ポリシーを有効にする] をクリックしてポリシーを作成し、有効にします。
- [ドラフトとして保存] をクリックして、ポリシーをドラフト状態で保存します。この場合、Carbon Black Cloud はポリシーを [無効] として保存します。ポリシーを編集して有効にできます。Kubernetes セキュリティ強化ポリシーの編集および Kubernetes セキュリティ強化ポリシー ドラフトを有効にするを参照してください。

次のステップ

Kubernetes セキュリティ強化ポリシーを構成したら、[Kubernetes ワークロード] 画面の [ワークロードの詳細] ペインでルール違反を確認できます。

適用する事前設定

Carbon Black によって、ルールの適用事前設定を作成して、リソースにアクションを適用できます。事前設定は事前定義済みの要件で、組織の基準から逸脱するリソースを自動的に変更することで、特定のフィールドと値を適用します。

DevSecOps は、既存のリソースの構成セットを変更して会社が導入した要件を満たすのではなく、ルールを適用することで、環境を制御し、違反の数を減らすことができます。

Kubernetes セキュリティ強化ポリシーへの適用事前設定の割り当て

Kubernetes セキュリティ強化ポリシーに適用事前設定を追加するには、次の手順を実行します。

注： この手順では、[適用] - [K8s ポリシー] 画面で [セキュリティ強化ポリシー] タブを使用します。または、[ルール] タブで適用事前設定をルールに割り当てることができます。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 ポリシーの名前をクリックして、ポリシーの編集や新しいポリシーの追加を行います。コンテナ イメージの Kubernetes カスタム ルールの作成および Kubernetes セキュリティ強化ポリシーの編集を参照してください。

4 [次へ] をクリックします。

5 [ルールの追加] 画面で、[適用] オプションを含むルールを見つけて、[適用] を選択します。

ルールでユーザー入力が必要な場合は、[適用事前設定] ドロップダウン メニューが表示されます。

6 事前設定をルールに割り当てるには、次のいずれかを実行します。

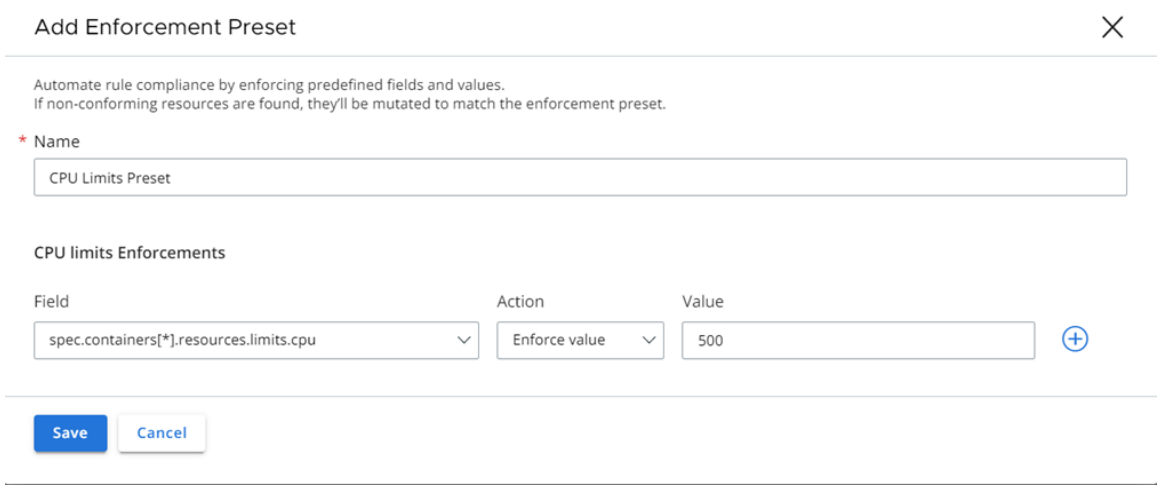
- [適用事前設定] ドロップダウン メニューから既存の事前設定を選択します。
- [新しい事前設定を追加] をクリックして、新しい事前設定を作成します。

7 新しい事前設定を作成するには、[新しい事前設定を追加] をクリックします。

a 事前設定の名前を入力し、[フィールド] ドロップダウン メニューからルール固有のフィールドを選択します。

b [アクション] ドロップダウン メニューからアクションを選択し、適用値を入力します。

フィールドをさらに追加するには、プラス [+] アイコンをクリックします。



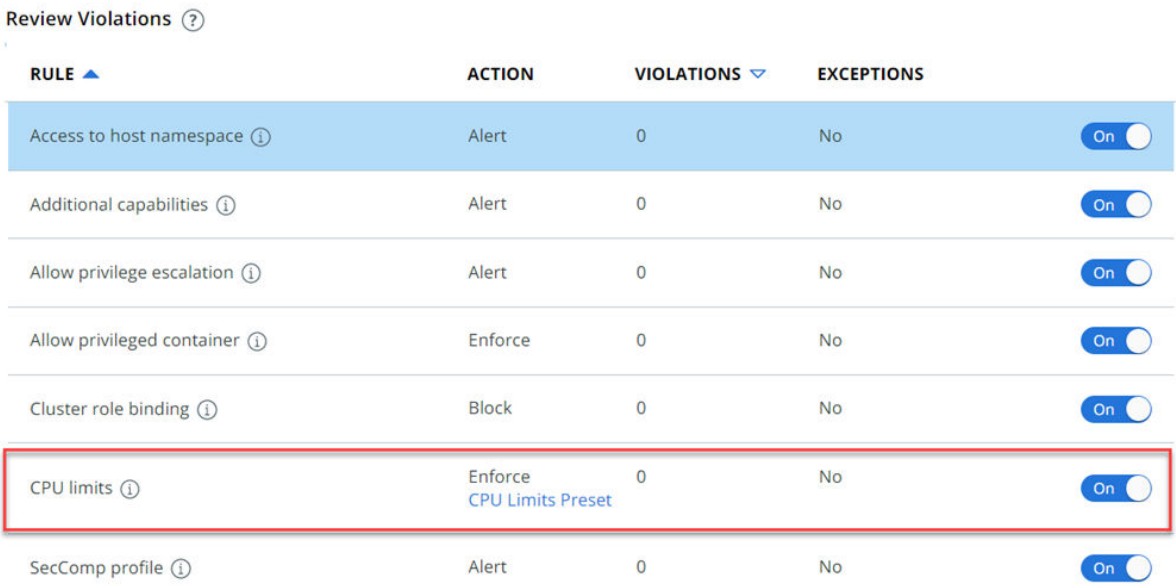
c [保存] をクリックします。

新しく定義された事前設定が [適用事前設定] ドロップダウン メニューに表示されます。

8 ポリシーにルールを追加するには、ルールの右側にあるキャレット  アイコンをクリックします。

9 [次へ] をクリックします。

変更したルールが [違反の確認] セクションに表示され、ルールの適用事前設定名が [アクション] 列に表示されます。



新しいリソースが展開されると、システムは事前定義されたフィールドを使用して適用されます。

10 [保存] をクリックします。

適用事前設定の追加または削除

適用事前設定を追加または削除するには、次の手順を実行します。

注： 現在使用中の事前設定は削除できません。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

3 適用事前設定を持つルールを見つけてダブルクリックします。

4 右側の [ルールの詳細] ペインで、[適用事前設定] ドロップダウン メニューをクリックします。

このルールで使用可能なすべての事前設定が表示されます。

5 適用事前設定を見つけて、ドロップダウン メニューをクリックし、アクションを選択します。

- 事前設定の値フィールドを更新するには、[編集] を選択し、変更内容を保存します。
- 事前設定を削除するには、[削除] を選択し、操作を確定します。

注： ポリシーで事前設定が使用されている場合、ドロップダウン メニューは無効になります。

結果

事前設定を編集した後、既存のワークロードは環境に再展開されるまで変更されません。

Kubernetes セキュリティ強化ポリシーの編集

Kubernetes セキュリティ強化ポリシーを編集するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 ポリシー名をクリックして編集するか、[アクション] ドロップダウン メニューで [ポリシーを編集] をクリックします。

注： ランタイム ポリシーのフィールドとルールの詳細については、Kubernetes ランタイム ポリシーおよび Kubernetes ランタイム ポリシーの作成を参照してください。

a ポリシーがリンクされている範囲を変更し、[次へ] をクリックします。

b 必要に応じてルールを追加または削除し、[次へ] をクリックします。

注： 適用事前設定を変更または追加するには、Kubernetes セキュリティ強化ポリシーへの適用事前設定の割り当てを参照してください。

c ポリシーの詳細を確認して、[保存] をクリックします。

注： 環境内の問題が解決されるまで、違反が多すぎる場合は、ルールを無効にできます。ポリシーからルールを除外するには、ルールの状態を `Off` に切り替えます。

Kubernetes セキュリティ強化ポリシー ドラフトを有効にする

[無効] になっている Kubernetes ポリシーを有効にできます。[無効] 状態のポリシーは、作成時にドラフトとして保存されました。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 [無効] ステータスのポリシーを選択し、[アクション] ドロップダウン メニューで [ポリシーを有効にする] をクリックします。

結果

ポリシーがすぐに有効になります。

セキュリティ強化ポリシーをテンプレートとして保存

Kubernetes セキュリティ強化ポリシーのルールを保存して他のポリシーで使用するには、ポリシーをテンプレートとして保存します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 選択したポリシーについて、 [アクション] ドロップダウン メニューで [テンプレートとして保存] をクリックします。

4 新しいテンプレートの名前を入力し、[保存] をクリックします。

結果

新しく作成したテンプレートが保存されます。[テンプレート] タブが [Kubernetes ポリシー] 画面に表示され、新しいテンプレートに焦点を合わせます。Kubernetes ポリシー テンプレートを参照してください。

セキュリティ強化ポリシーの複製

Kubernetes セキュリティ強化ポリシーの同じルール構成を別の範囲で使用するには、 ポリシーを複製します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 選択したポリシーについて、 [アクション] ドロップダウン メニューで [複製] をクリックします。

4 新しいテンプレートの名前を入力し、[保存] をクリックします。

新しいポリシーを作成するためのウィザードには、元のポリシーのすべてのデータが入力されます。

5 ポリシー名と範囲を変更し、複製されたポリシーを保存します。

Kubernetes ポリシー ルール

ルールは、Kubernetes ポリシーの主要コンポーネントです。ルールは Kubernetes リソースに適用されます。事前定義されたルールを使用したり、カスタム ルールを作成したりできます。

- 組み込みルールは、Kubernetes セキュリティ構成に基づいています。これらはカテゴリに分割され、事前定義されたテンプレートで使用されます。
- カスタム ルールは、Kubernetes ワークロードまたはコンテナ イメージのユーザー定義ルールです。カスタム ルールを更新すると、ルールが適用されるすべてのポリシーに変更が影響します。

セキュリティ強化ポリシー ルールの表示

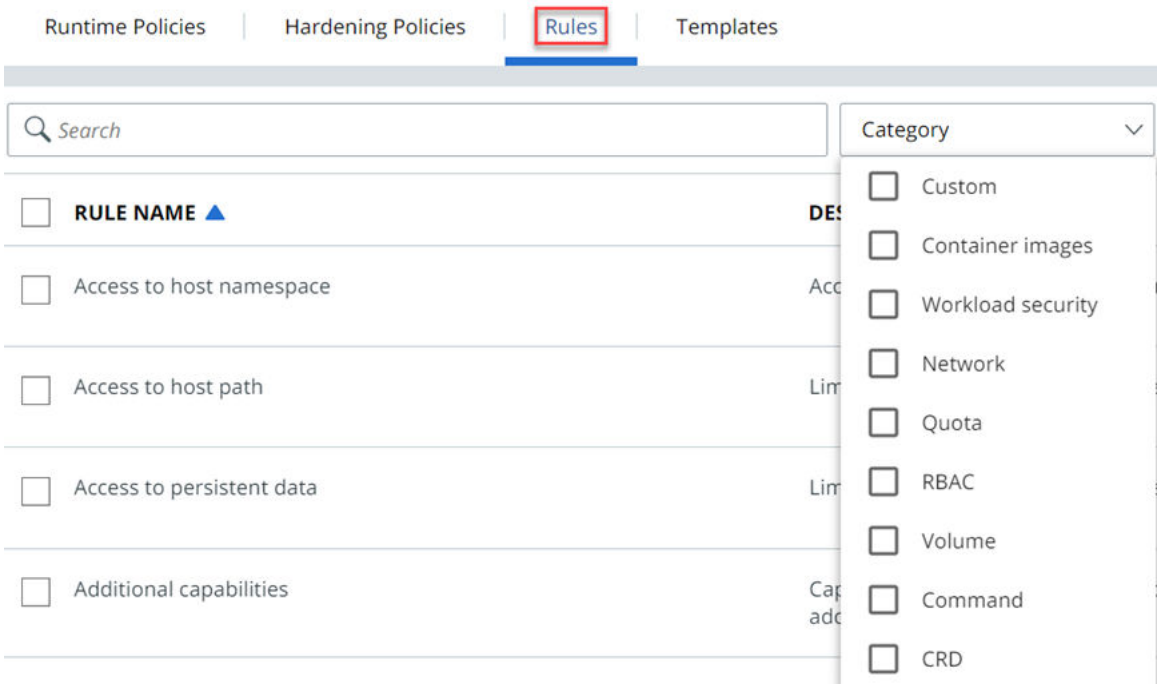
既存のセキュリティ強化ポリシー ルールを表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

ルールのリストは、カテゴリ別にフィルタリングできます。



テンプレートへのセキュリティ強化ルールの追加

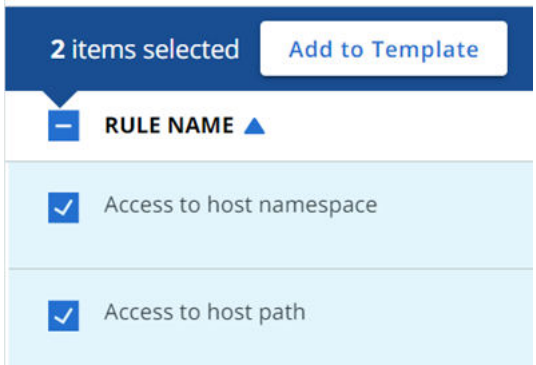
セキュリティ強化ポリシー ルールをテンプレートに追加するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

3 テンプレートに追加するルールを選択します。



4 [テンプレートに追加] をクリックしドロップダウン リストからテンプレートを選択します。

5 [保存] をクリックします。

組み込みの Kubernetes ポリシー ルール

このトピックでは、Kubernetes セキュリティ強化ポリシーの組み込みルールについてアルファベット順に一覧表示します。

組み込みルール

ルール名	説明	カテゴリ
ホスト名前空間へのアクセス	ホストのネットワーク、PID、および IPC 名前空間へのアクセス。	ワークロード セキュリティ
ホストパスへのアクセス	コンテナでのホスト ディレクトリの使用を制限します。	ボリューム
永続データへのアクセス	非コア ボリューム タイプの使用を PersistentVolumes で定義されたボリューム タイプに制限します。	ボリューム
追加機能	この機能により、バイナリの「root/non-root」二分法がきめ細かいアクセス制御システムに変わります。このルールは、コンテナの実行時に追加される機能を適用するのに役立ちます。	ワークロード セキュリティ
権限の昇格を許可	AllowPrivilegeEscalation は、プロセスが親プロセスよりも多くの権限を取得できるかどうかを管理します。	ワークロード セキュリティ
特権コンテナを許可	コンテナを特権モードで実行します。特権コンテナ内のプロセスは、基本的にホストの root と同じです。	ワークロード セキュリティ
AppArmor	AppArmor (Application Armor) は、オペレーティング システムとそのアプリケーションをセキュリティ上の脅威から保護する Linux セキュリティ モジュールです。これを使用するには、システム管理者が AppArmor セキュリティ プロファイルを各プログラムに関連付けます。	ワークロード セキュリティ
クラスタ ロールのバインド	ユーザーまたはサービス アカウントをクラスタ内のロールとそのすべての名前空間にバインドします。	RBAC
会社の禁止リスト	会社の禁止ファイルを含むイメージの展開を防止します。	コンテナ イメージ
CPU 制限	ワークロード間で CPU を分散し、単一のコンテナがリソースを使い果たしてシステムを停止できないようにします。	割り当て
クリティカルな脆弱性	OS パッケージまたはライブラリに重大な脆弱性があるイメージの展開を防止します。	コンテナ イメージ
一時コンテナを拒否	一時コンテナは、ポッド コンテキスト内でアドホック コンテナを実行することで、ツール セットまたはアクセスが制限されたワークロードをデバッグするのに役立ちます。管理者にとっては強力ですが、一時コンテナは攻撃者が悪意を持ってワークロードへの特権アクセスを取得するために使用する可能性があります。	コマンド
最新のタグを拒否	「最新」タグを持つコンテナ イメージを識別します。最新のタグを使用すると、イメージ バージョンの追跡や適切なロールバックが困難になります。	コンテナ イメージ
新しいリソースを拒否	関連付けられた範囲内の新しいリソースの展開を特定します。	ワークロード セキュリティ
新しい CRD の展開	特定の Kubernetes インストールをカスタマイズして、Kubernetes リソースを拡張します。カスタム リソースがインストールされると、ユーザーは kubectl を使用してオブジェクトを作成してアクセスできます。	CRD
ルートなしの適用	コンテナは、root プライマリまたは補助 GID で実行しないようにする必要があります。コンテナのユーザー/グループ ID を指定するか、runAsNonRoot を true に設定すると、コンテナは root 以外のユーザーまたはグループとして実行する必要があることを示します。	ワークロード セキュリティ

ルール名	説明	カテゴリ
Exec からコンテナ	Kubectl exec を使用すると、ユーザーはコンテナでコマンドを実行できます。権限を持つ攻撃者が「kubectl exec」を実行して、悪意のあるコードを実行し、クラスタ内のリソースを侵害する可能性があります。	コマンド
ホスト ポート	ホスト ポートによってワークロードを公開できるようにします。	ネットワーク
イメージがスキャンされない	展開から 20 分以内にスキャンされていないイメージを含むワークロードを特定します。	コンテナ イメージ
入力方向コントローラ	入力方向コントローラによってワークロードを公開できるようにします。	ネットワーク
既知のマルウェア	既知のマルウェアを含むイメージの展開を防止します。	コンテナ イメージ
ロード バランサ	ロード バランサによってワークロードを公開できるようにします。	ネットワーク
メモリ制限	ワークロード間でメモリを分散し、単一のコンテナがリソースを使い果たしてシステムを停止できないようにします。	割り当て
ノード ポート	ノード ポートによってワークロードを公開できるようにします。	ネットワーク
ポート転送	Kubectl ポート転送を使用すると、クラスタの境界セキュリティをバイパスし、localhost の内部 Kubernetes クラスタ プロセスと直接やり取りできます。	コマンド
ハッシュ タグを要求	名前付きタグを持つコンテナ イメージを特定します。名前付きタグの上書きによる問題を防ぐには、ハッシュ タグが必要です	コンテナ イメージ
ロールのバインド	ユーザーまたはサービス アカウントを名前空間内のロールにバインドします。	RBAC
SecComp プロファイル	このコンテナで使用される seccomp オプション。seccomp オプションがポッド レベルとコンテナ レベルの両方で指定されている場合、コンテナ オプションはポッド オプションより優先されます。	ワークロード セキュリティ
シークレットの検出	シークレットを持つイメージの展開を防止します。	コンテナ イメージ
SeLinux	コンテナに適用される SELinux コンテキスト。指定しない場合、コンテナ ランタイムは各コンテナにランダムな SELinux コンテキストを割り当てます。	ワークロード セキュリティ
Sysctl	Sysctls は、ポッドに使用される namespaced sysctls のリストを保持します。サポートされていない sysctls を持つポッド（コンテナ ランタイムによって）の起動に失敗することがあります。	ワークロード セキュリティ
Unmasked proc mount	ProcMount は、コンテナに使用する proc mount のタイプを示します。デフォルトでは、読み取り専用パスとマスクされたパスにコンテナ ランタイムのデフォルトが使用されます。	ワークロード セキュリティ
修正による脆弱性	修正が利用可能な場合は、中、高、または重大な脆弱性を含むイメージの展開を防止します。	コンテナ イメージ
書き込み可能ファイル システム	ファイルへの書き込みを許可することで、脅威を取り込みやすくなり、環境内で持続しやすくなります。	ワークロード セキュリティ

組み込みルールの仕様

注： 組み込みルールの仕様表の幅のため、HTML でのみ表示できます。組み込みポリシー ルールの [組み込みルールの仕様] を参照してください。

Kubernetes セキュリティ強化ポリシーのカスタム ルール

このセクションの概念と手順を使用して、Kubernetes セキュリティ強化ポリシーのカスタム ルールを作成します。

各ルール タイプについては、個別のトピックで説明します。共通の特性は以下のとおりです。

特性	説明
名前	ルールの名前は一意である必要があります
説明	ルールの簡単な説明。この情報は、Carbon Black Cloud コンソールのいくつかの場所に表示されます。 ■ [適用] > [K8s ポリシー] > [ルール] ■ [適用] > [K8s ポリシー] > [テンプレート] ■ [適用] > [K8s ポリシー] > [セキュリティ強化ポリシー] > [ポリシーの追加] > [違反の確認]

基本的な JSONPath ルール

カスタム ルールを追加するための JSONPath オプションは、機能が制限された管理可能なアクセス制御ポリシー言語 (MAPL) ルールのガイド付き構成です。MAPL は、マイクロサービス環境でのアクセスを制御するルールの言語です。この種類のルールを使用して、Kubernetes リソースに必要な状態を定義します。

JSONPath カスタム ルールには、論理演算子にリンクされた複数の条件を組み込めます。条件には、想定される値に接続されている Kubernetes リソース（[リソースの種類]）が含まれます。

基本的な JSONPath カスタム ルールは、 コンソールのガイド付き構成を使用して構成できます。

特性	説明
リソースの種類	ルールが参照する Kubernetes リソースのタイプ。
JSONPath	JSONPath セレクタは、特定の設定を取得し、Kubernetes リソースの構成ファイル内で値を指定するために使用されます。 **注：** **$** 記号を使用した [JSONPath] セレクタ文字列を開始する必要があります。 カスタム ルールでは、AND ロジックを使用して個々のリソースを照合する複数の JSONPath 条件を設定できます。 JSONPath は、JSON または YAML ファイルの要素または選択要素を示すパスです。JSON パス式は、ツリーとして作成されます。 `{.element} {.child} {.grand-child}` JSON パス式はドット (.) で始まります。構成のルートとの照合を開始するには、その後に子、孫などの名前を入力します。 `[:]` を使用して、配列内の任意の要素 (例: `$.metadata.labels` 内のラベル名など) を照合します。例： `$*.metadata.labels[:].name*`。

特性	説明
メソッド	リソース値を評価する方法: ■ EQ - 等しい ■ NE- 等しくない ■ RE - 正規表現と一致する ■ NRE - 正規表現と一致しない ■ LT - 未満 ■ LE - 以下 ■ GT - 超 ■ GE - 以上 ■ EX - 存在する ■ NEX - 存在しない ■ IN - 値のリスト内 [val1,val2,val3,...] ■ NIN - 値のリストにない [val1,val2,val3,...]
値	リソース値と一致するしきい値。値が一致しない場合、ルールに違反します。

例： JSON の例

```
{
  "apiVersion": "v1",
  "kind": "Namespace",
  "metadata": {
    "creationTimestamp": "2021-04-09T00:52:44Z",
    "managedFields": [
      {
        "apiVersion": "v1",
        "fieldsType": "FieldsV1",
        "fieldsV1": {
          "f:status": {
            "f:phase": {}
          }
        },  ...
```

例： カスタム ルール 1 の例

5 個以上のレプリカを持つワークロードを許可しないでください。

```
$.spec.replicas GT 5
```

例： カスタム ルール 2 の例

すべてのコンテナに対して CPU が割り当てられている必要があります。

```
$.spec.template.spec.containers[:].resources.limits.cpu NEX
```

例： カスタム ルール 3 と 4 の例

各ワークロードに `serviceOwner` というラベルと、メール アドレスのように見える値 (2 つのルール) がある必要があります。

- `$.spec.template.metadata.label.serviceOwner NEX`

- `$.spec.template.metadata.label.serviceOwner NRE .+@example\.com`

JSONPath Kubernetes カスタム ルールの作成

Carbon Black Cloud コンソールには、JSONPath 基準を作成および検証するためのオプションの手順がいくつか用意されています。

正しい JSONPath セレクタを構築するには、サンプル リソース構成を入力するか、Kubernetes 環境に展開済みのリソースの構成をインポートできます。この構成に基づいて、Carbon Black Cloud コンソールにセレクタの結果のプレビューが表示され、セレクタを構築できます。

前提条件

基本的な JSONPath ルールを参照してください。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

3 [ルールの追加]をクリックします。

4 ルールを定義します。

   a 一意のカスタム ルール名と説明を入力します。

   b ルール基準に [JSONPath、メソッド、値] を選択します。

   c [次へ] をクリックします。

5 必要に応じて、ドロップダウン メニューから [リソースの種類] を入力します。デフォルト値は [任意] です。

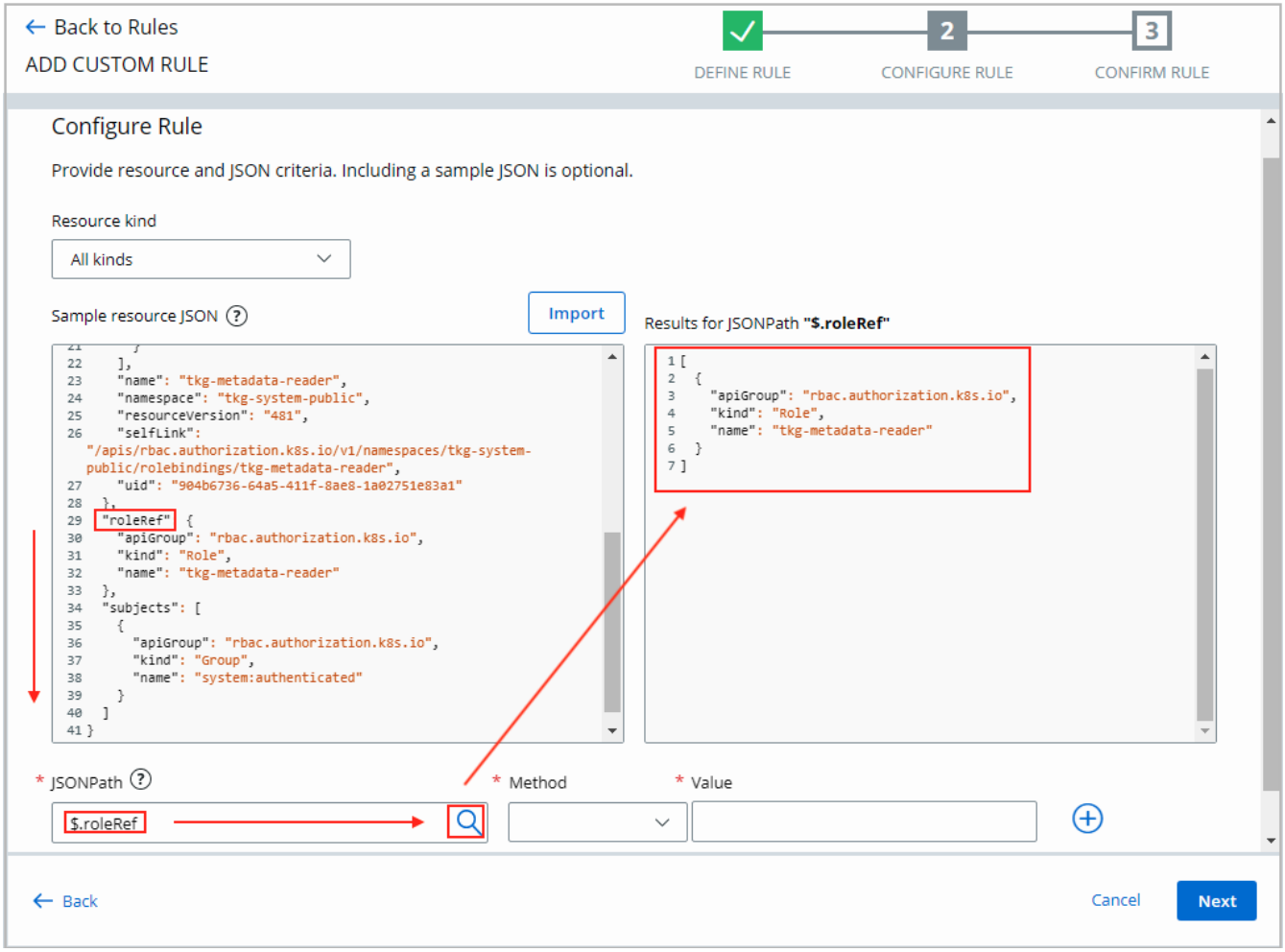
6 [インポート] をクリックして、Kubernetes 環境から既存のリソース ファイルを開きます。[サンプル リソース JSON] テキスト ボックスにコンテンツをコピーして貼り付けることもできます。

   リソース ファイルまたはコピーしたコンテンツは、画面の左側の [サンプル リソース JSON] テキスト ボックスに表示されます。

7 [JSONPath] で、表示されている JSON ファイルからコピーできる文字列を入力し、テキスト ボックスの右側にある  アイコンをクリックします。

8 ドロップダウン メニューから [メソッド] を入力し、[値] に入力します。

9 画面の右側にある [JSONPath の結果] 領域で選択内容をプレビューします。入力した文字列がリソースを返さない場合は、その旨のメッセージが表示されます。[1] など、数字が表示された場合は、一致するリソースが 1 つ表示されます。



10 [次へ] をクリックします。

11 [ルールの確認] 画面で、ルール基準と一致する Kubernetes リソースのサマリを確認し、[保存] をクリックします。

カスタム ルールが [ルール] 画面に追加されます。詳細を確認するには、ルールの右側にある矢印

アイコンをクリックします。

コンテナ イメージの Kubernetes カスタム ルールの作成

組み込みルールに基づくコンテナ イメージのカスタム ルールを作成できます。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

3 [ルールの追加]をクリックします。

4 ルールを定義します。

a 一意のカスタム ルール名と説明を入力します。

b ルール基準として [コンテナ イメージ基準] を選択します。

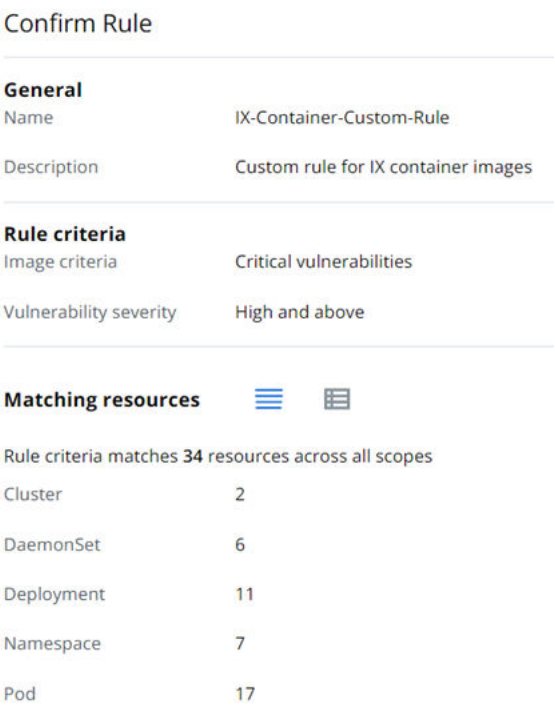
c [次へ] をクリックします。

5 ルールを構成します。次のオプションがあります。

イメージ基準	脆弱性の重要度またはレジストリ ドメイン
[クリティカルな脆弱性] **注：** 重要度が「クリティカル」の脆弱性は、デフォルトの[クリティカルな脆弱性]の組み込ルールの一部です。[クリティカル (9.0 ～ 10.0)] を選択した場合は、既存の組み込みルールを複製します。	■ クリティカル (9.0 ～ 10.0) ■ 高以上 (7.0 ～ 10.0) ■ 中以上 (4.0 ～ 10.0) ■ 低以上 (0.1 ～ 10.0)
[修正による脆弱性]	■ クリティカル (9.0 ～ 10.0) ■ 高以上 (7.0 ～ 10.0) ■ 中以上 (4.0 ～ 10.0) ■ 低以上 (0.1 ～ 10.0)
[許可されたレジストリ]	ソースとして許可するレジストリを指定します。例えば、**`docker.io`** です。

6 [次へ] をクリックします。

7 [ルールの確認] 画面で、ルール基準と一致する Kubernetes リソースのサマリを確認し、[保存] をクリックします。



高度な Kubernetes カスタム ルールの作成

高度な Kubernetes カスタム ルールを作成するには、YAML ファイルを使用して、Kubernetes リソースの MAPL ルールと適用可能な条件を説明します。

YAML 形式の MAPL ルールは、Kubernetes 環境のためにカスタム ルールを構成する方法をより具体的に規定します。

前提条件

高度なカスタム ルールを正常に構成するには、Kubernetes 環境に適用可能な MAPL 言語で記述された YAML ファイルが必要です。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [ルール] タブをクリックします。

3 [ルールの追加]をクリックします。

4 ルールを定義します。

   a 一意のカスタム ルール名と説明を入力します。

   b ルール基準として [高度 - MAPL アクセス コントロール ルール (YAML 形式)] を選択します。

   c [次へ] をクリックします。

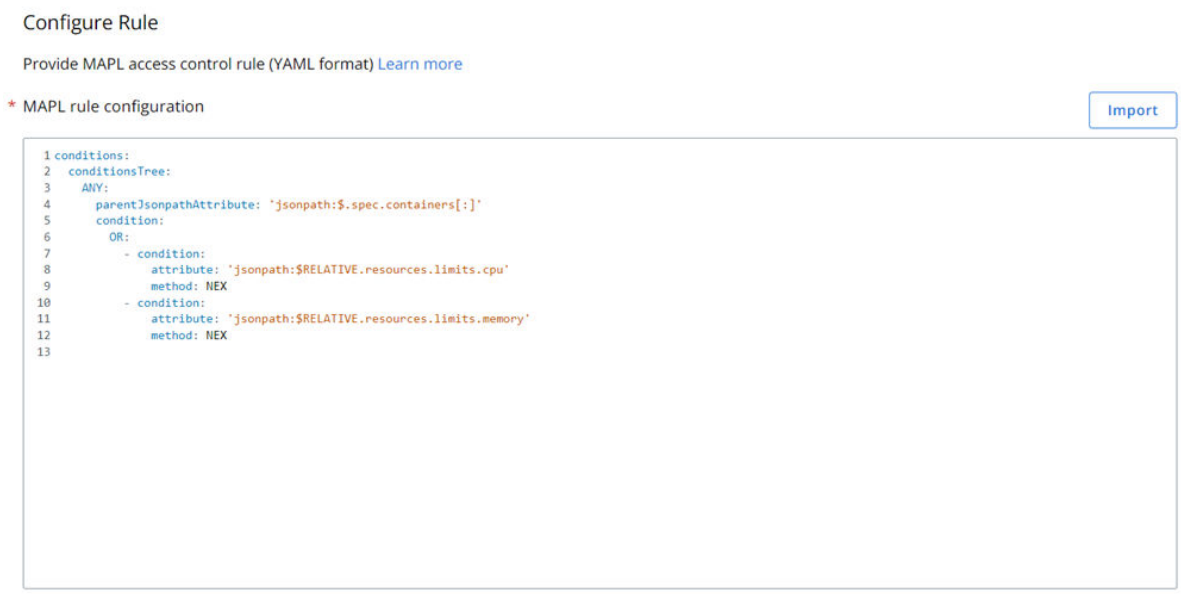
5 テキスト領域に YAML コードを入力するか、[インポート] をクリックして YAML ファイルをインポートします。

注：

- YAML ファイルには、Kubernetes 構成データに対してテストされた論理素子を使用して、1 つの属性条件を含める必要があります。
- 属性は JSONpath です。
- メソッドは次のいずれかです（値は固定値です）。

EQ - 等しい	EX - 存在する	GE - 以上
GT - 超	IN - 値のリスト内 [val1,val2,val3,...]	LE - 以下
LT - 未満	NE- 等しくない	NEX: 存在しない
NIN - 値のリストにない [val1,val2,val3,...]	NRE - 正規表現と一致しない	RE - 正規表現と一致する

例：



MAPL（管理可能なアクセス制御ポリシー言語）（外部リンク）を参照してください。

6 [次へ] をクリックします。

7 [ルールの確認] 画面で、ルール基準と一致する Kubernetes リソースのサマリを確認し、[保存] をクリックします。

Kubernetes カスタム ルールの編集または削除

Kubernetes カスタム ルールを編集または削除するには、次の手順を実行します。

注：

- カスタム ルールは、Kubernetes セキュリティ強化ポリシーに含まれる場合でも、作成後に編集できます。
- カスタム ルールが Kubernetes セキュリティ強化ポリシーの一部である場合、削除できません。

手順

1. 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。
2. [ルール] タブをクリックします。
3. 編集するルールを見つけて、行の最後にある矢印  アイコンをクリックします。
4. 右側のパネルのドロップダウン メニューで、アクションを選択します。
   - ルールをテンプレートに追加するには、[テンプレートに追加] をクリックし、1 つ以上のカスタム テンプレートを選択し、[保存] をクリックします。
   - ルールを更新するには、[編集] をクリックします。[カスタム ルールの編集] ウィンドウが表示されます。ルール タイプは変更できません。[次へ] をクリックし、構成ウィザードの手順に従ってルールを変更します。[保存] をクリックします。
   - ルールを複製するには、[複製] をクリックします。新しいルールの名前を変更してカスタマイズします。
   - ルールを削除するには、[削除] をクリックし、[OK] をクリックして削除を確定します。

Kubernetes セキュリティ強化ポリシー ルールの例外の作成

Kubernetes セキュリティ強化ポリシーを作成または更新するときに違反を確認できます。また、ルールの例外を作成して違反の数を減らすことができます。例外を作成すると、ルール アクションからワークロードが除外されます。

重要： Carbon Black では、既知の動作を示す特定のワークロードを除外する例外のみを作成することをお勧めします。例外を考慮する前に、できるだけ多くの違反を修正してください。

ヒント: 環境内の問題が解決されるまで、違反が多すぎる場合は、ルールを無効にできます。ポリシーからルールを除外するには、ルールの状態を `Off` に切り替えます。

手順

1. 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。
2. [セキュリティ強化ポリシー] タブをクリックします。
3. 編集するポリシー名をクリックします。
4. [次へ] を 2 回クリックして [違反の確認] 画面に移動します。

5 [アラート] または [適用] アクションを持つルールを選択し、[例外] タブをクリックします。

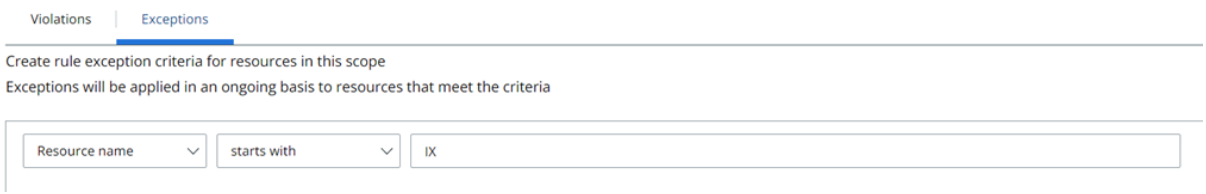
6 [条件を追加] をクリックします。

7 [リソース名] ドロップダウン メニューで例外基準を定義します。オプションは次のとおりです。

- [リソース名]: [次と同じ]、[次で始める]、または [次で終わる] に設定します。名前の基準を入力します。

  特定のワークロード、または同じプリフィックスやサフィックスを持つワークロードなど、複数のワークロードに一致する基準を指定できます。

- [ワークロード ラベル]: キーと値のペアを定義します。
- [ユーザー名]: 入力した名前と [同じ] になります。



例外基準は、ポリシー範囲の一部である現在および将来のワークロードと一致します。

8 [追加] をクリックします。

注： 例外を削除するには、例外基準の横にあるゴミ箱アイコン をクリックします。

結果

違反の総数は減少します。ルール違反から除外されたワークロードは、[例外] タブに表示されます。

セキュリティ強化ルールの変更

選択したリソース プロパティの値を適用して、問題を一時的に修正できます。ルールの [適用] アクションを設定すると、変更された値が考慮され、違反アラートが表示されます。修正後もワークロードがルールに違反している場合、展開はブロックされます。

注： このコンテキストで、変更は、ポリシーが新しい基準に基づいて Kubernetes リソースを変更することを意味します。たとえば、権限のエスカレーションを許可します。

[適用] アクションを適用できるルールは、次の表に記載されています。

ルールカテゴリ	適用アクションを許可するルール	リソース フィールド	適用される値
ワークロードセキュリティ	ホスト名前空間へのアクセス	spec.hostNetwork	False
		spec.hostPID	
		spec.hostIPC	
	権限の昇格を許可	spec.containers[*].securityContext.allowPrivilegeEscalation	False
	特権コンテナを許可	spec.containers[*].securityContext.privileged	False
	書き込み可能ファイル システム	spec.containers[*].securityContext.readOnlyRootFilesystem	True
	SecComp プロファイル	metadata.annotations['container.seccomp.security.alpha.kubernetes.io/*']	ユーザー定義
		metadata.annotations['seccomp.security.alpha.kubernetes.io/pod*']	
		spec.securityContext.seccompProfile.type	
		spec.containers[*].securityContext.seccompProfile	
	Sysctl	spec.securityContext.sysctls	ユーザー定義
	追加機能	spec.containers[*].securityContext.capabilities.add	ユーザー定義
	AppArmor	metadata.annotations['container.apparmor.security.beta.kubernetes.io/*']	ユーザー定義
	Unmasked proc mount	spec.containers[*].securityContext.procMount	空白（フィールドを削除）

ルールカテゴリ	適用アクションを許可するルール	リソース フィールド	適用される値
	ルートなしの適用	spec.securityContext.runAsNonRoot	ユーザー定義のユーザーおよびグループ ID
		spec.containers[*].securityContext.runAsNonRoot	
		spec.containers[*].securityContext.runAsGroup	
		spec.containers[*].securityContext.runAsUser	
		securityContext.runAsGroup	
		securityContext.runAsUser	
クオータ	CPU 制限	spec.containers[*].resources.limits.cpu	ユーザー定義
		spec.containers[*].resources.requests.cpu	
	メモリ制限	spec.containers[*].resources.limits.memory	ユーザー定義
		spec.containers[*].resources.requests.memory	

ルールの結果の変更

ポリシーの作成中に、ルールの [適用] アクションを設定できます。このアクションは、事前定義された値をルールの結果に設定します。ユーザー定義の値が必要な適用ルールの事前設定を選択する必要があります。

前提条件

[適用] アクションを許可するルールのリストについては、セキュリティ強化ルールの変更を参照してください。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 編集するポリシー名をクリックするか、[アクション] ドロップダウン メニューで [編集] をクリックします。

4 [次へ] をクリックします。

5 [ルールの追加] 画面で、右側のペインの [ルールの追加] を確認するか、中央ペインで [ワークロード セキュリティ] カテゴリまでスクロールします。

6 セキュリティ強化ルールの変更の表にリストされている各ルールに対して、[適用] アクションを選択します。

7 [次へ] を 2 回クリックし、[保存] をクリックします。

結果

セキュリティ標準に準拠するようにルールのプロパティ値を設定しました。違反はトリガされません。

Kubernetes ポリシー テンプレート

Kubernetes ポリシー テンプレートは、例外が含まれていない事前定義済みルールまたはカスタム ルールのグループです。

事前定義済みのルール設定には、次のカテゴリが含まれています。

カテゴリ	目的
コマンド	Kubernetes コマンドラインのコマンドを制限します
コンテナ イメージ	コンテナ イメージの脆弱性を特定します
CRD	カスタム リソースの使用量を制限します
カスタム	システムに存在するすべてのカスタム ルール
ネットワーク	サービス タイプが Kubernetes の外部に公開されないようにします
割り当て	CPU およびメモリの割り当て容量
RBAC	幅広い権限を持つ新しいロールを制限します
ボリューム	データへのアクセスを制限します
ワークロード セキュリティ	Kubernetes セキュリティ構成に基づくルール。ポッドのセキュリティ基準（外部リンク）を参照してください。

Kubernetes ポリシー テンプレートの作成

Kubernetes セキュリティ強化ポリシーで再利用するために、特定のルールをカスタム テンプレートでグループ化できます。カスタム テンプレートは、組み込みルールとカスタム ルールの組み合わせです。これらは、ポリシーを作成するときに適用されます。

注： ポリシーで [アラート] または [ブロック] アクションを構成しますが、テンプレートでは構成しません。したがって、異なるアクションを持つ異なるポリシーに同じルールを設定できます。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [テンプレート] タブをクリックします。

3 [テンプレートの追加] をクリックします。

4 カスタム テンプレートの名前を入力し、[保存] をクリックします。

テンプレートが作成され、[カスタム テンプレート] のリストに表示されます。

5 新しく作成したカスタム テンプレートにルールを追加するには、[オプション] > [テンプレートの編集] の順にクリックします。

6 カスタム テンプレートに追加するルールを選択します。

7 [保存] をクリックします。

セキュリティ強化ポリシーをテンプレートとして保存

Kubernetes セキュリティ強化ポリシーのルールを保存して他のポリシーで使用するには、ポリシーをテンプレートとして保存します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

3 選択したポリシーについて、 [アクション] ドロップダウン メニューで [テンプレートとして保存] をクリックします。

4 新しいテンプレートの名前を入力し、[保存] をクリックします。

結果

新しく作成したテンプレートが保存されます。[テンプレート] タブが [Kubernetes ポリシー] 画面に表示され、新しいテンプレートに焦点を合わせます。Kubernetes ポリシー テンプレートを参照してください。

アラート通知のサブスクライブ

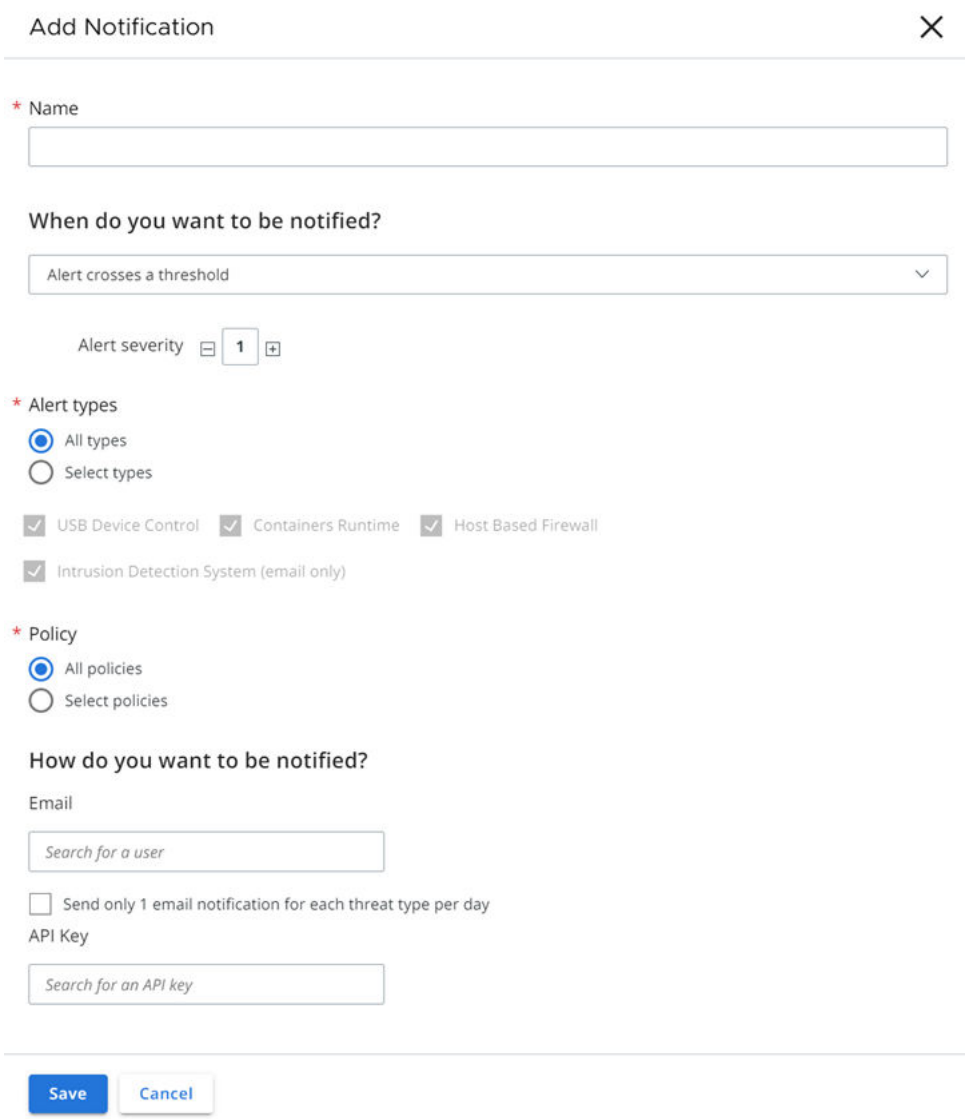
アラートが発生したときに通知を受信するには、次の手順を実行します。

前提条件

メール アドレスは、登録済みの Carbon Black Cloud コンソール ユーザーに関連付ける必要があります。

手順

1 左側のナビゲーション ペインで、[設定] - [通知] の順にクリックします。



2 [通知の追加] をクリックし必須テキスト フィールドに入力します。

a ドロップダウン メニューから [アラートがしきい値を超えています] という通知タイプを選択します。この設定は、アラートが指定された重要度のしきい値を超えた場合に通知します。

b アラートの重要度のしきい値を指定します。

c 通知を受信するアラート タイプを選択します。デフォルト値は [すべてのタイプ] です。

d すべてのポリシーまたは特定のポリシーを選択します。[すべてのポリシー] がデフォルト値です。

複数のポリシーを選択すると、Carbon Black Cloud コンソールはポリシーごとに別々に通知を送信します。

e 通知の取得方法を選択します。

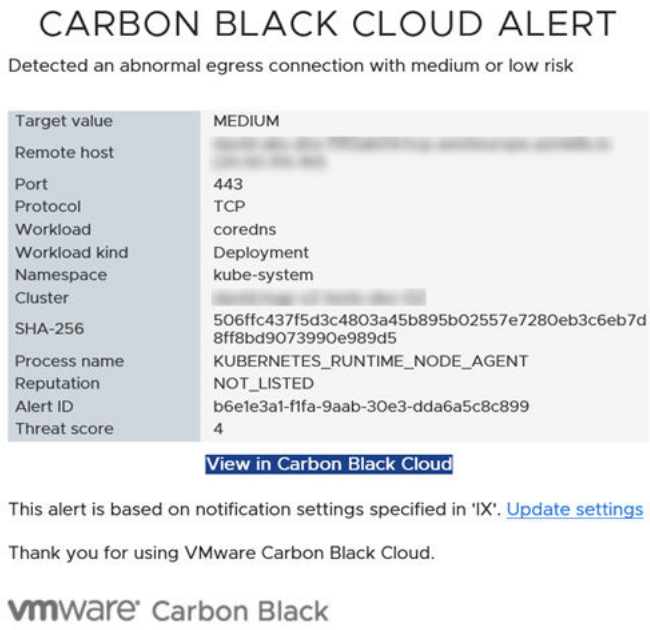
[E メール] オプションまたは [API キー] のいずれかを選択します。どちらのオプションでも、1 人以上のユーザーを選択します。

f オプション。受信する E メールの数を減らすには、[脅威のタイプごとに 1 日あたり 1 通の E メール通知のみを送信] チェック ボックスを選択します。

3 [保存] をクリックします。

結果

通知は、[通知リスト] に表示されます。通知条件に一致するアラートが浮上すると、通知メールが送信されます。例：


CARBON BLACK CLOUD ALERT

Detected an abnormal egress connection with medium or low risk

Target value	MEDIUM
Remote host	[redacted]
Port	443
Protocol	TCP
Workload	coredns
Workload kind	Deployment
Namespace	kube-system
Cluster	[redacted]
SHA-256	506ffc437f5d3c4803a45b895b02557e7280eb3c6eb7d8ff8bd9073990e989d5
Process name	KUBERNETES_RUNTIME_NODE_AGENT
Reputation	NOT_LISTED
Alert ID	b6e1e3a1-f1fa-9aab-30e3-dda6a5c8c899
Threat score	4

View in Carbon Black Cloud

This alert is based on notification settings specified in 'IX'. Update settings

Thank you for using VMware Carbon Black Cloud.

vmware Carbon Black

API アクセスの設定

Carbon Black のオープン API プラットフォームを使用して、SIEM、チケット追跡システム、独自のカスタム スクリプトなど、さまざまなセキュリティ製品と連携できます。

連携パートナーを検索するには、https://www.vmware.com/products/vmware-marketplace.html をご覧になるか、Carbon Black Developer Network（https://developer.carbonblack.com/）にアクセスしてください。

ヒント: アクセス プロファイルと許可 API を使用して、組織内のプリンシパルのロールを管理（作成/読み取り/更新/削除）することもできます。

API キーの作成と管理

API キーを作成および管理してアクセス レベルを設定することで、サービス統合を環境に追加し管理します。

API キーを作成するときは、次の制限と影響を理解する必要があります。

- API 呼び出しの大部分には、「カスタム」タイプの API キーが必要です。その他のキー タイプはレガシーであり、段階的に廃止されています。このキー タイプは、Splunk アプリケーションおよび今後リリースされるその他の統合に必要です。アクセスを制限するには、必要な権限のみを持つアクセス レベルを作成します。
- SIEM タイプの API キーは通知 API からの通知のみ受け取ることができます。SIEM タイプの API キーを使用して Syslog コネクタを構成します。新しい統合では、使用可能なすべてのデータを受信するために次のいずれかを使用する必要があります。
  - データ フォワーダ: アラートまたはイベントを自分の S3 バケットにストリーミングし、保持を管理できます。
  - アラート v6 API: 最大 180 日間の履歴アラート データを検索します
- ポリシーと監査ログ API には API タイプのキーが必要です。
- [API Access (API アクセス)] ページの API ID と API 秘密鍵は、Carbon Black Cloud コンソールのログイン パスワードと同様に扱います。

前提条件

統合に [カスタム] アクセス権限を使用するには、アクセス レベルを作成する必要があります。

手順

1 左側のナビゲーション ペインで [設定] - [API アクセス] をクリックします。

2 [オプション]: API キーにカスタム アクセス レベルが必要な場合は、ここでそのアクセス レベルを作成します。

   a [アクセス レベル] タブをクリックします。

   b アクセス レベル名を指定します。

   c アクセス レベルの権限を指定します。

   詳細なガイドについては、Developer Network の「認証」セクションを参照してください。

3 [API キーを追加] をクリックします。

   a API キーに一意の名前と簡単な説明を入力します。

   b 適切なアクセス レベル タイプを選択します。

   注： カスタム アクセス レベルを使用するには、[アクセス レベル タイプ] ドロップダウン メニューから [カスタム] を選択し [カスタム アクセス レベル] を指定します。(手順 2 を参照。)

   c [オプション]: 承認された IP アドレスを追加します。

   セキュリティ上の理由から、API キーの使用を特定の IP アドレス セットに制限できます。

   注： 承認された IP アドレスは、カスタム キーでは使用できません。

4 変更を適用するには、[保存] をクリックします。

結果

ポップアップ ウィンドウに新しい API 認証情報が表示されます。これには、API ID と API セキュリティ キーが含まれます。

例

API ID: `F3HLZ13ZS3`

API セキュリティ キー: `FGD7T51232HQ37GN3VE8UZYF`

次のステップ

目的	アクション
特定の API キーの名前、説明、または IP アドレスを更新するには:	[アクション] 列の [編集] ボタンをクリックします。
特定の API キーの認証情報を表示するには:	[アクション] ドロップダウン メニューをクリックし、[API 認証情報] を選択します。
新しい認証情報を生成するには:	[アクション] ドロップダウン メニューをクリックし、[API 認証情報] を選択して [新しい API 秘密鍵の生成] をクリックします。 **注：** 統合を有効にするには、API 秘密鍵を再入力する必要があります。
時間枠内に API キーに送信されたすべての通知を表示するには:	[アクション] ドロップダウン メニューをクリックし、時間枠を選択します。
API キーの削除を確認するには:	[アクション] ドロップダウン メニューをクリックし、[削除] を選択します。 **注：** 通知ルールに関連付けられている API キーは削除できません。

通知ルールが関連付けられた API キーの削除

通知ルールが関連付けられた API キーを削除するには、最初に関連付けられたすべての通知ルールを削除し、次に API キーを削除する必要があります。

手順

1. Carbon Black Cloud コンソールにログインし、[Settings (設定)] - [API Access (API アクセス)]ページに移動します。
2. 削除する API キーの [API ID] を見つけます。
3. [Settings (設定)] - [Notifications (通知)] ページに移動します。
4. [Subscribers (加入者)] 列で API ID を見つけ、関連付けられているすべての通知ルールを削除します。
5. [Settings (設定)] - [API Access (API アクセス)] ページに移動し、API キーを削除します。

   API キーが [API Access (API アクセス)] ページから削除されました。

アクセス レベルの設定

アクセス レベルでは、他のセキュリティ製品と統合する場合に、アクセス レベルをカスタマイズできます。API キーに適用する特定の詳細な権限を持つカスタム アクセス レベルを作成します。

アクセス レベルの作成

API を使用して Carbon Black Cloud 統合のデータにアクセスするには、API に適したアクセス レベルを決定する必要があります。

手順

1 左側のナビゲーション ペインで [設定] - [API アクセス] をクリックします。

2 [アクセス レベル] タブをクリックし、[アクセス レベルの追加] をクリックします。

3 アクセス レベルの名前と説明を入力します。

4 アクセス レベルに含める許可機能のボックスを選択します。

5 [保存] をクリックします。

結果

新しく作成されたアクセス レベルは、[アクセス レベル] タブに表示できます。

次のステップ

アクセス レベルを変更または削除するには、[アクション] 列を使用します。アクセス レベルをエクスポートする場合は、ロール定義の詳細を含む JSON ファイルをダウンロードします。

API キーへのアクセス レベルの適用

統合へのアクセス権を付与するときに、API キーにカスタム アクセス レベルを適用します。

注： テスト目的でのみ、[カスタム アクセス レベル] ドロップダウン メニューからユーザー ロールを選択します。ユーザー ロールにはバージョン管理されていない API が含まれる場合があります。現在サポートされバージョン管理されているすべての API の詳細については、Carbon Black Developer Network を参照してください。

前提条件

カスタム アクセス レベルを作成します。「アクセス レベルの作成」「」を参照してください。

手順

1 左側のナビゲーション ペインで [設定] > [API アクセス] をクリックします。

2 [API キー] タブを選択し、[API キーを追加] をクリックします。

3 API キーの名前と簡単な説明を入力します。

4 [アクセス レベル タイプ] ドロップダウン メニューから [カスタム] を選択します。

5 組織で使用可能なユーザー ロールまたはアクセス レベルを [カスタム アクセス レベル] ドロップダウン メニューから選択します。

6 変更を適用するには、[保存] を選択します。

結果

新しく作成された API キーが [API キー] タブに表示されます。

次のステップ

[アクション] 列を使用して API キーを編集するか、ドロップダウン メニューを使用して、関連付けられている API キー認証情報と通知履歴を表示します。

イメージのスキャン

4

コンテナ イメージの既知の脆弱性をスキャンし、Carbon Black Cloud コンソールでシステム クラスタのスキャンまたは手動スキャンの結果を確認できます。

注：

- イメージ スキャンは、Linux オペレーティング システム パッケージに基づくイメージにのみ適用されます。
- イメージ スキャンには CLI クライアントが必要です。イメージ スキャン用 CLI クライアントの設定を参照してください。

コンテナ イメージは、次の状況でスキャンされます。

- スキャンは、継続的インテグレーション/継続的展開 (CI/CD) パイプラインまたは手動スキャンによってトリガされます。コンテナ イメージの手動再スキャンを参照してください。
- Kubernetes センサー バージョンの更新。Kubernetes センサーのアップグレードを参照してください。
- クラスタのセットアップ時のコンテナ イメージの初期クラスタ スキャン。クラスタの追加と Kubernetes センサーのインストールを参照してください。
- Carbon Black Cloud 脆弱性データベースの新しい脆弱性。
- ファイルのレピュテーションを更新しました。

クラスタ イメージ スキャンには、次のメリットがあります。

- 環境内のコンテナ イメージの可視性。
- 見つかった脆弱性と使用可能な修正に関する情報。
- イメージ スキャン レポート内からイメージ レベルで例外を作成する機能。
- Kubernetes ポリシーにより、重大な脆弱性を持つコンテナ イメージが CI/CD パイプラインを介して進行するのを防ぎます。Kubernetes ポリシーを参照してください。
- 展開されたすべてのイメージとマルウェア検出のファイル レピュテーション スキャン。コンテナ イメージ内のマルウェアの検出を参照してください。

  ファイル レピュテーションに関する最新情報を取得するには、サードパーティのフィード プロバイダから取得したファイル レピュテーション データを更新し、新しく展開されたイメージのクラスタを一貫して再スキャンする必要があります。

次のトピックを参照してください。

コンテナ イメージの手動再スキャン

コンテナ イメージのスキャンは、Carbon Black Cloud コンソールまたは CLI クライアントを使用してターミナルで実行できます。次の手順では、Carbon Black Cloud コンソールでイメージ スキャンを実行します。

コンテナ イメージが構築され、パブリック リポジトリにプッシュされ、2 回のスキャンの間に Kubernetes クラスタに展開されている場合、[保留] ステータスでリストに表示されます。イメージ スキャンのステータスが [エラー] の場合は、CLI クライアントを使用して、Carbon Black Cloud コンソールまたはターミナルでそのイメージのスキャンを実行できます。

注： 手動スキャンは、パブリック リポジトリ内のイメージに対してのみ実行できます。イメージがプライベート リポジトリに属している場合、[再スキャン] ボタンは非アクティブです。

前提条件

CLI クライアントをダウンロードして構成します。イメージ スキャン用 CLI クライアントの設定を参照してください。ターミナルで CLI クライアントを使用するには、Container Security API および統合（外部リンク）を参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

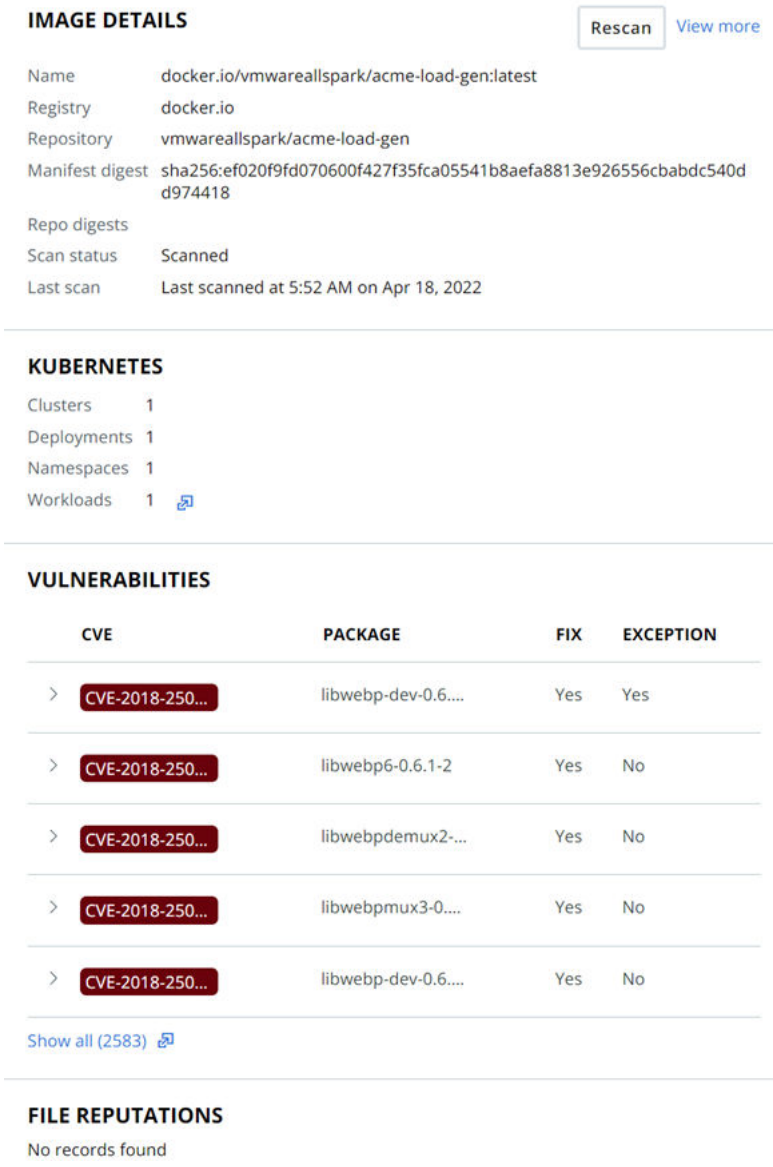
2 [展開されたイメージ] タブを選択します。

3 縮小されている場合は、左上のキャレット [>>] をクリックしてフィルタ オプションを展開します。[スキャン ステータス] フィルタで、[Error] を選択します。

表には、[エラー] ステータスのイメージのみが表示されます。

4 検索フィールドを使用して特定のイメージを検索するか、リストからコンテナ イメージを選択します。選択したイメージの右側にある矢印  アイコンをクリックします。

5 [イメージの詳細] パネルで [再スキャン] をクリックします。



コンテナの監視と分析

5

ロールとユーザーを作成し、Kubernetes クラスタを設定し、範囲とポリシーを構成したら、システムを使用して動作を監視および分析する準備が整います。

次のトピックを参照してください。

- 重要度スコアリング
- コンテナ イメージの監視
- コンテナ イメージでのファイル レピュテーションの管理と表示
- シークレットの検出と防止
- Kubernetes ワークロードの監視
- ネットワーク アクティビティの分析

重要度スコアリング

このセクションでは、コンテナで使用される 2 種類のセキュリティ スコアリングの方法について説明します。

Kubernetes リスクの重要度スコアリング

リスクの重要度は、Kubernetes ワークロードのセキュリティ脆弱性のリスクを表すメトリックです。これは、構成ミスに関連するセキュリティ リスクを評価するためのフレームワークである Kubernetes 共通構成評価システム (KCCSS) を使用します。

注： Kubernetes ワークロードのリスク評価は、さまざまな基準で評価されるため、コンテナ イメージの脆弱性のリスクの重要度とは異なります。コンテナ イメージのリスク スコアの詳細については、コンテナ イメージのリスク評価を参照してください。

Kubernetes 共通構成評価システム

KCCSS は、リスクと修正の両方を個別のルールとして評価します。ワークロードのすべてのランタイム設定のリスクと、ワークロードの全リスクを計算します。ワークロードごとに、0 (リスクなし) から 10 (高リスク) までのリスク スコア範囲が割り当てられます。

リスクの測定

KCCSS は、次の 3 つの領域で、リスクのある構成の潜在的な影響を示します。

機密性

個人を特定できる情報 (PII) の漏洩、キーへのアクセスの可能性など。

整合性

ランタイム動作の変更、新しいプロセスの起動、新しいポッドなどを可能にするような、コンテナ、ホスト、またはクラスタへの不要な変更。

可用性

リソース枯渇、サービス拒否など。

KCCSS は、リスクがコンテナに限定されるか、それともクラスタ全体に影響を与えるか、リスクの悪用のしやすさ、攻撃にローカル アクセスが必要かどうかを考慮します。ワークロードに関連するすべてのセキュリティ リスクと、ワークロードに対する全体的なリスク スコアを示すために必要な修正を組み合わせます。

リスク スコア

評価システムは、Kubernetes 構成の 30 を超えるセキュリティ設定を考慮しています。正確なルールと評価方式は、KCCSS の一部です。スコアに基づいて、ワークロードは重要度 (高、中、低) のレベルでフィルタリングされます。リスク スコアが高いほど、重要度が高くなります。すべてのワークロードに 0（リスクなし）～10（高リスク）のリスク スコアが割り当てられます。

スコアの範囲	重要度
0 ～ 3	低
4 ～ 6	中
7 ～ 10	高

コンテナ イメージのリスク評価

共通脆弱性評価システム (CVSS) は、ソフトウェアの脆弱性の特性と重要度を説明するための標準の測定システムです。すべての脆弱性に 0.0（リスクなし）～ 10.0（最大リスク）のリスク スコアが割り当てられます。

注： ワークロードはさまざまな基準で評価されるため、コンテナ イメージの脆弱性に対するリスク評価と、ワークロードのリスクの重要度は異なります。Kubernetes ワークロードのリスク スコアの詳細については、Kubernetes リスクの重要度スコアリングを参照してください。

CVSS は、次の 3 つの測定基準グループで構成されます。

- [基本]: 長い時間ユーザー環境全体で一定である脆弱性の特性。
- [一時的]: 時間の経過とともに変化する可能性はあるが、ユーザー環境には広がらない脆弱性の特性。
- [環境]: 特定のユーザー環境に関連する、固有の脆弱性の特性。

詳細については、共通脆弱性評価システム SIG（外部リンク）を参照してください。

リスク スコアの範囲と重要度は次のように定義されています。

評価	スコア
なし	0.0
低	0.1 ～ 3.9
中	4.0 ～ 6.9
高	7.0 ～ 8.9
クリティカル	9.0 ～ 10.0

注： 脅威ベクトルがまだ分かっていない脆弱性は、[不明] の重要度にグループ化されます。これは、システムが特定のアーティファクトを脆弱性として識別できたが、脆弱性に CVE が付加されていない可能性があることを意味します。不明の重要度は、0 ～ 10 の範囲である可能性があります。

イメージの脆弱性評価のカラー インジケータ

共通脆弱性評価システム (CVSS) は、検出された脆弱性の重要度を推定するために使用されます。CVSS で定義されているリスク スコアに加えて、[不明] カテゴリが Carbon Black Cloud コンソールに表示されます。

CVSS の詳細については、コンテナ イメージのリスク評価を参照してください。

さまざまな Carbon Black Cloud コンソール画面に、さまざまな脆弱性リスク スコアのカラー バーが表示されます。カラー バーは次の評価に対応しています。

カラー名	カラー バー	評価 (CVSS を参照)
緑		なし
黄		低
オレンジ		中
赤		高
エンジ色		クリティカル
グレイ		不明

カラー バー内の数字は、脆弱性の数/修正回数を示しています。

注： ワークロードはさまざまな基準で評価されるため、コンテナ イメージの脆弱性に対するリスク評価と、ワークロードのリスクの重要度は異なります。Kubernetes ワークロードのリスク スコアの詳細については、Kubernetes リスクの重要度スコアリングを参照してください。

コンテナ イメージの監視

コンテナは、軽量でポータブルな実行可能イメージです。コンテナ イメージは、継続的統合環境のビルドまたは展開ステージにあります。

このセクションでは、コンテナ イメージのデータを監視および分析する方法について説明します。

コンテナ イメージの表示 - 概要

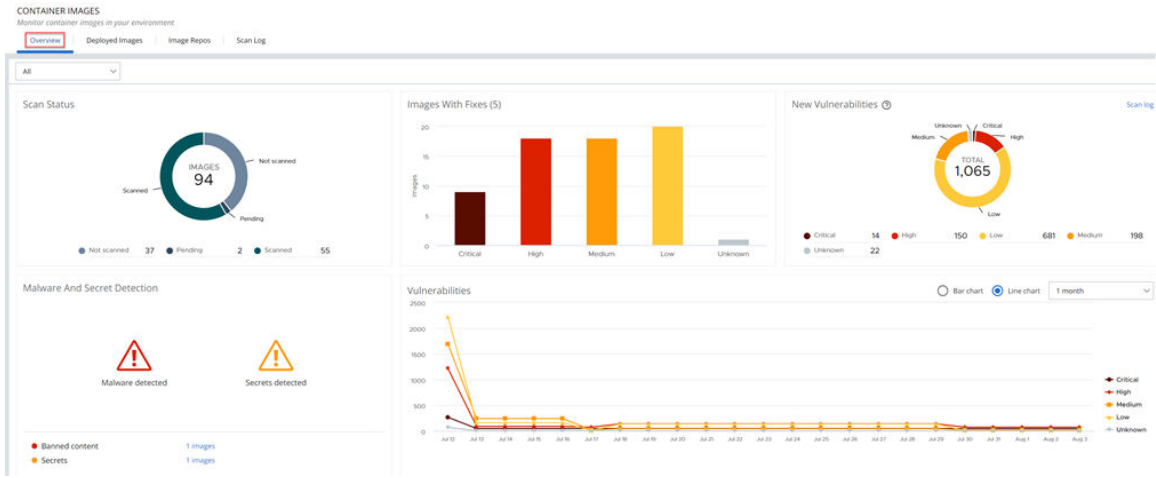
このトピックでは、Carbon Black Cloud コンソールの [コンテナ イメージ] 画面で取得できるコンテナ イメージ データの概要について説明します。

手順

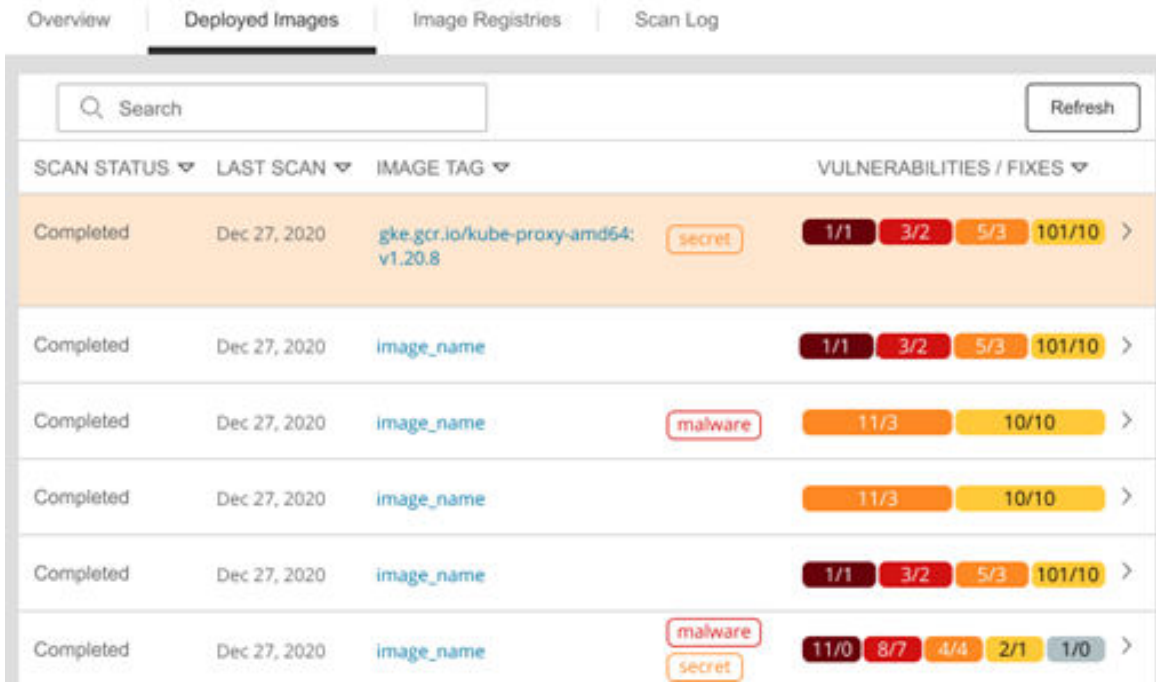
- 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。
  - Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
  - 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

  [コンテナ イメージ] 画面には、次のタブと情報が含まれています。

  - [概要] タブには、次の詳細が表示されます。



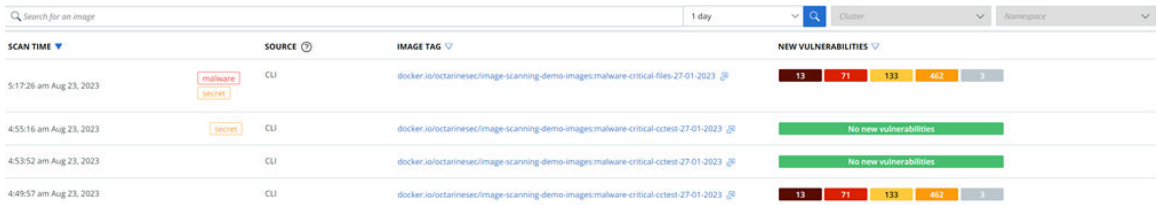
    - 最新のスキャン ステータスのサマリ
    - 新しい脆弱性
    - 修正による脆弱性
    - マルウェアとシークレットの検出
    - 指定された時間枠内に検出されたすべての脆弱性を示す棒グラフまたは折れ線グラフ
  - [展開されたイメージ] タブは、Kubernetes クラスタで実行されているコンテナ イメージのインベントリを表示し、脆弱性スキャンの結果と各イメージで使用可能な修正が含まれています。



[展開されたイメージ] タブで、以下を実行できます。

- 詳細なコンテナ データの表示 — [イメージ タグ] をクリックします。
- ワークロードに関する情報を表示 — [ワークロード] 列のリンク アイコンをクリックします。
- イメージの詳細を表示 — 行の右側にある矢印  アイコンをクリックします。展開されたコンテナ イメージの詳細の表示を参照してください。

- [イメージ リポジトリ] タブは、コンテナ イメージが存在するリポジトリのインベントリを表示します。リポジトリ内のすべてのイメージが表示されます。これには、使用されなくなった古いタグ、まだ展開されていないイメージ、展開されているイメージが含まれます。
- [スキャン ログ] タブには、検索可能なスキャン アクティビティが表示されます。例：



エントリの [イメージ タグ] をクリックすると、スキャン結果の詳細を表示できます。イメージ スキャン レポートの表示 - スキャン ログの詳細を参照してください。

展開されたコンテナ イメージの詳細の表示

展開されたイメージ スキャンと脆弱性の詳細を表示するには、次の手順を実行します。

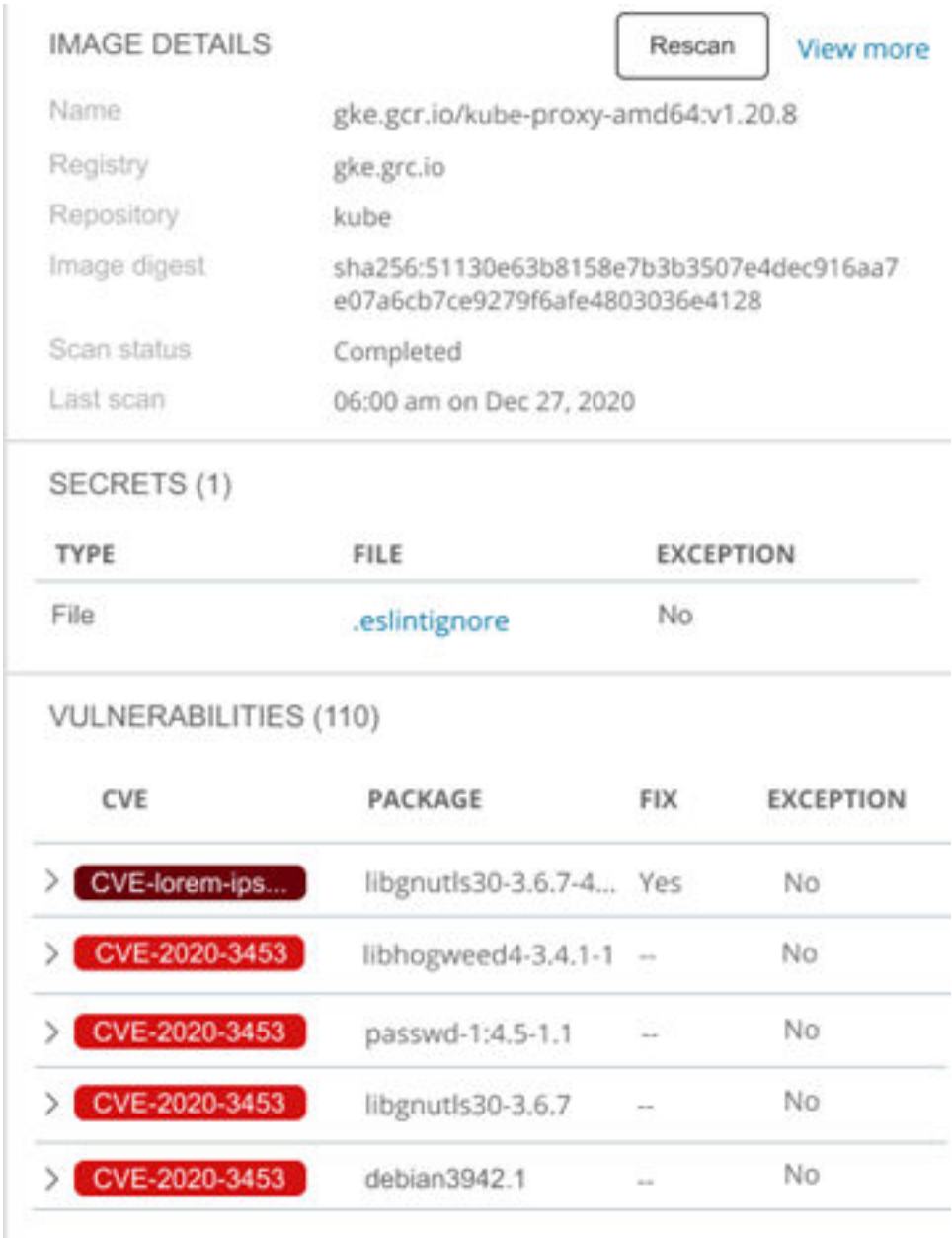
手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

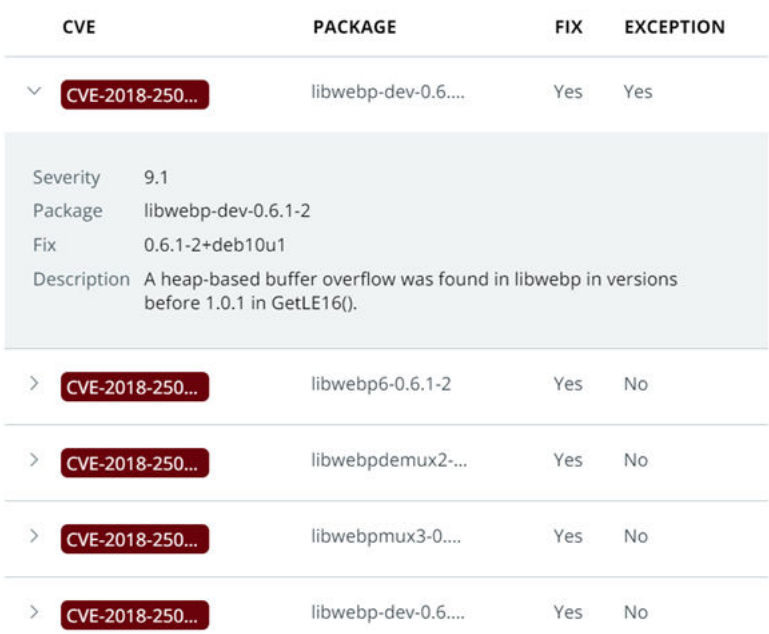
2 [展開されたイメージ] タブを選択します。

3 [イメージの詳細] パネルを展開するには、行の右側にある矢印  アイコンをクリックします。

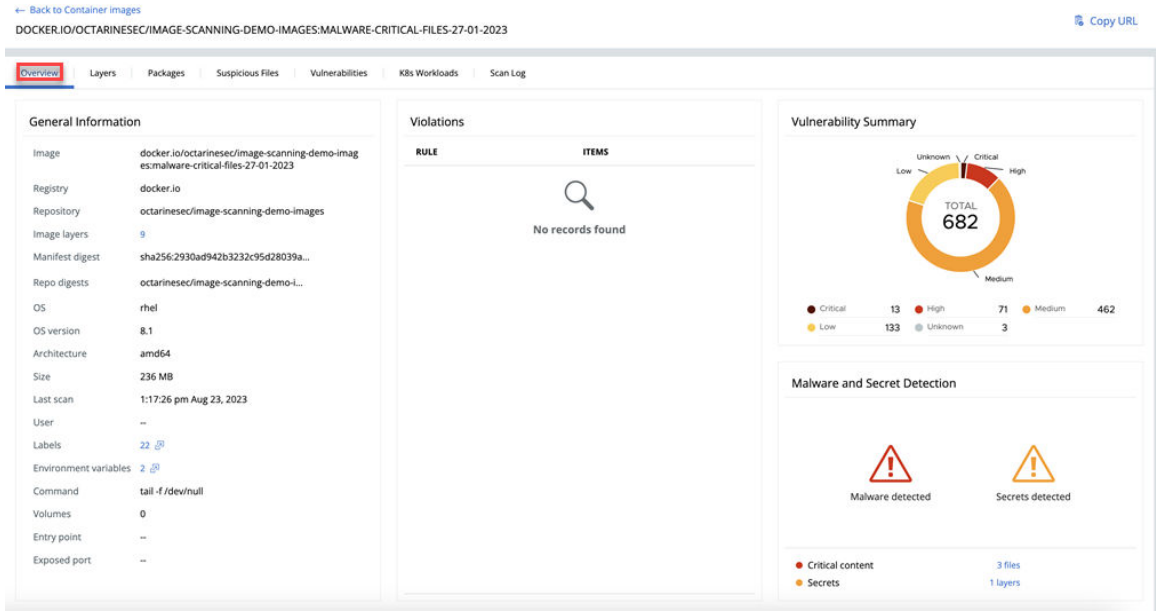


- イメージを再スキャンするには、[再スキャン] をクリックします。コンテナ イメージの手動再スキャンを参照してください。
- Kubernetes ワークロードの詳細を表示するには、[Kubernetes] セクションの[ワークロード] の横にあるリンク アイコンをクリックします。

- シークレットを含むファイルに関する情報にアクセスするには、[シークレット] セクションでファイル名をクリックします。
- 脆弱性が特定された CVE コードとパッケージの簡単な説明を表示するには、[CVE] の左側にあるキャレット  アイコンをクリックします。

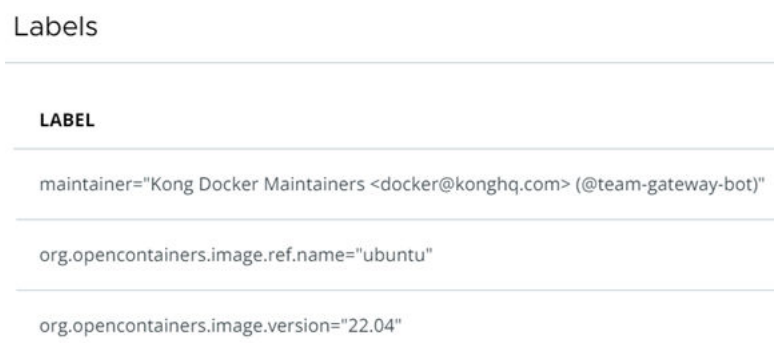


- このコンテナのすべての脆弱性を表示するには、[脆弱性] セクションのリンク アイコンをクリックします。コンテナ イメージの脆弱性の調査を参照してください。
- 展開されたイメージに関するその他の詳細を表示するには、[イメージの詳細] セクションで [詳細を表示] をクリックします。[イメージ スキャン レポート] 画面の [概要] タブが開きます。



4 シークレットに関する追加情報は、次の方法で表示できます。

- [ラベル] アイコンをクリックします。例：



- [環境変数] アイコンをクリックします。例：

コンテナ イメージ リポジトリの表示

イメージ リポジトリを表示するには、次の手順を実行します。

手順

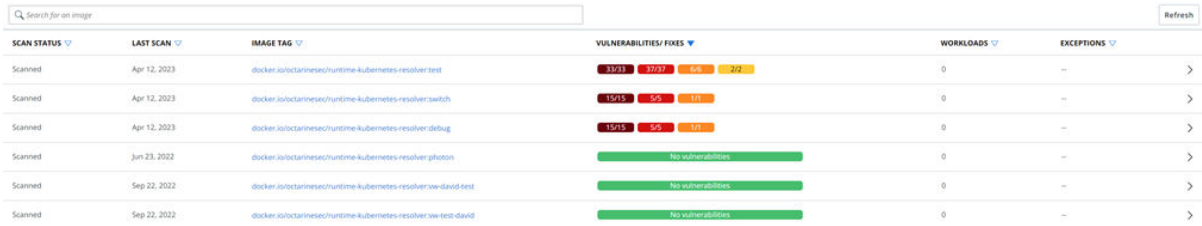
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [イメージ リポジトリ] タブをクリックします。

リポジトリとそのレジストリのリストが表示されます。リストを並べ替えたり、特定のリポジトリまたはレジストリを検索したりできます。

3 リポジトリの詳細を表示するには、[リポジトリ] 列でその名前をクリックします。



a イメージの [コンテナ イメージ] 画面を開くには、[イメージ タグ] 列でその名前をクリックします。

b イメージの詳細を表示するには、行の右側にある矢印  アイコンをクリックします。展開されたコンテナ イメージの詳細の表示を参照してください。

イメージ スキャン レポートの表示 - スキャン ログの詳細

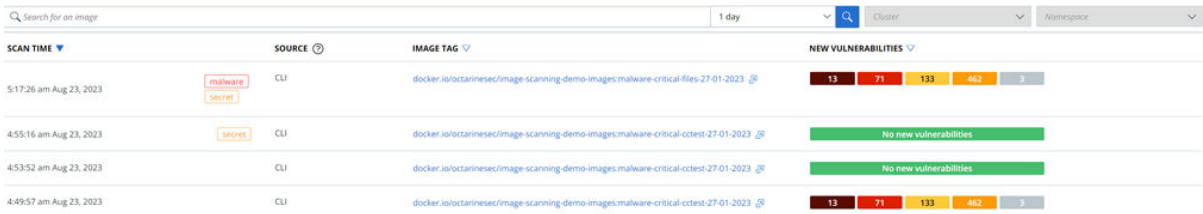
Carbon Black Cloud コンソールですべてのイメージ スキャンのスキャン ログを表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [スキャン ログ] タブを選択します。

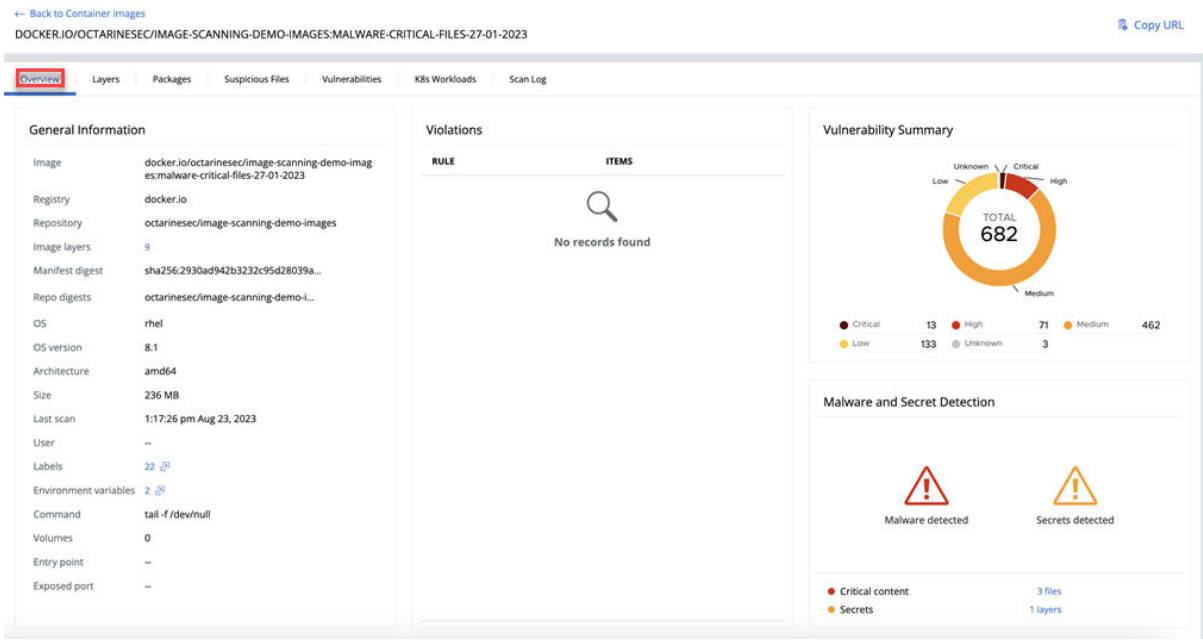


[送信元] 列は、スキャンが開始された理由を定義します。

送信元の列	説明
CLI	CI/CD パイプラインまたは手動スキャンによってトリガされたスキャン。
クラスタの再スキャン	Kubernetes センサー バージョンの更新。
クラスタのスキャン	Carbon Black Cloud コンソールで設定した Kubernetes クラスタにあるコンテナ イメージの初期クラスタ スキャン。
フィードの更新	Carbon Black Cloud 脆弱性データベースの新しい脆弱性に基づくイメージ スキャン。
レピュテーションの更新	ファイルのレピュテーションを更新しました。

3 イメージの詳細については、[イメージ タグ] アイコンをクリックします。

このアクションにより、[イメージ スキャン レポート] の [概要] タブが開きます。



コンテナ イメージ スキャン レポートを表示を参照してください。

コンテナ イメージ スキャン レポートを表示

コンテナ イメージのスキャン レポートを確認し、次のアクションを計画できます。[イメージ スキャン レポート] には、イメージ スキャンのすべての側面に関する完全な情報が表示されます。

前提条件

4 章 イメージのスキャンを参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。デフォルトでは、[概要] タブが開きます。

コンテナ イメージ スキャン レポートの表示 - 概要

コンテナ イメージのスキャン レポートを確認し、次のアクションを計画できます。[イメージ スキャン レポート] には、イメージ スキャンのすべての側面に関する完全な情報が表示されます。

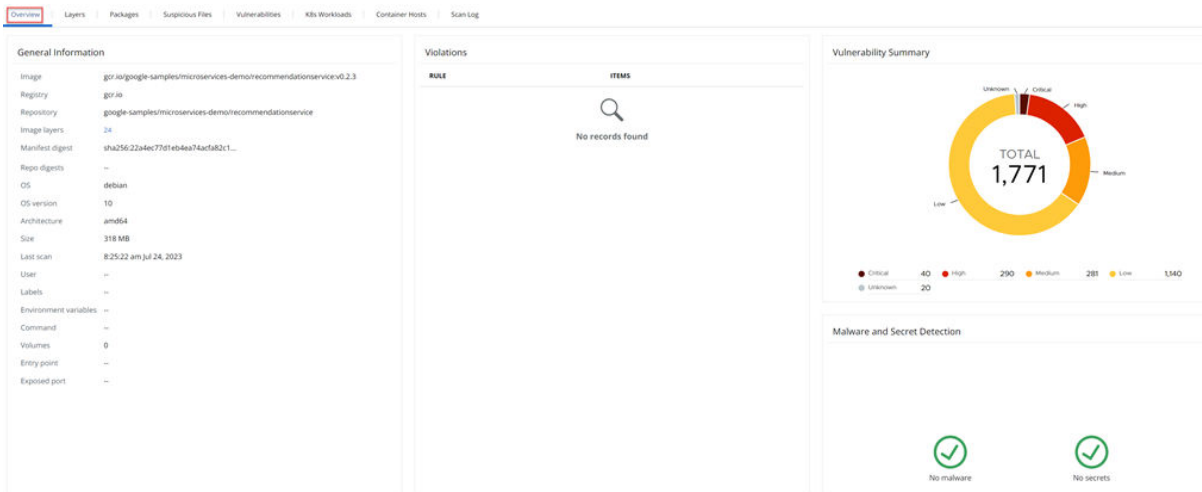
手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。デフォルトでは、[概要] タブが開きます。

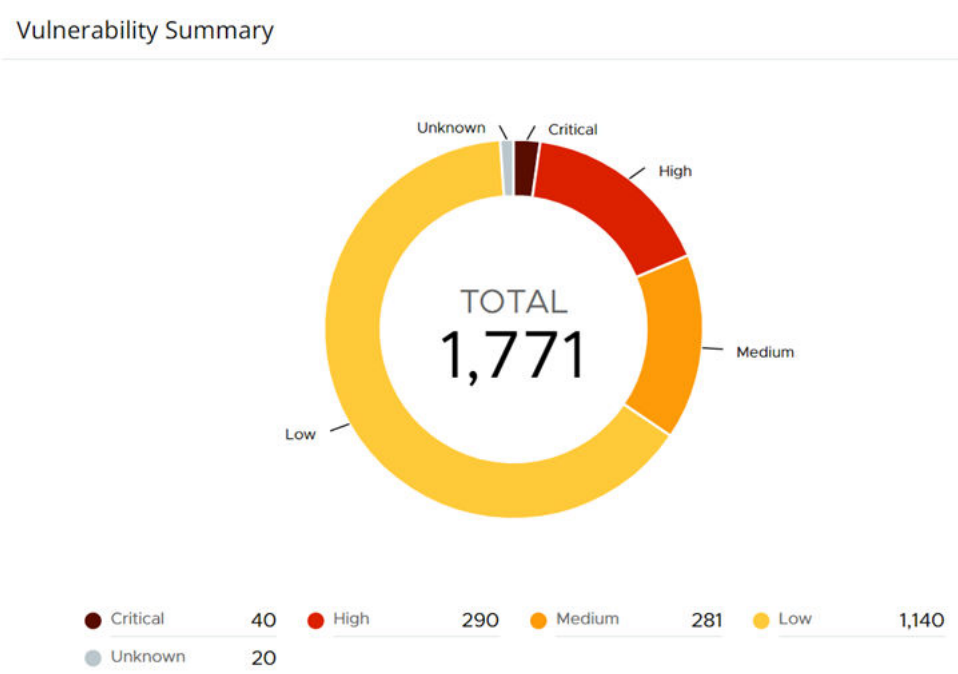


[一般情報] セクションには、基本的なコンテナ イメージ データが一覧表示されます。

イメージ名	レジストリ	リポジトリ
イメージ レイヤー: レイヤー番号は、このレポートの [レイヤー] タブにリンクします。コンテナ イメージ スキャン レポートの表示 - レイヤーを参照してください。	マニフェストのダイジェスト	レポのダイジェスト
オペレーティング システム	オペレーティング システムのバージョン	アーキテクチャ
サイズ	前回のスキャン日時	ユーザー
ラベル	環境変数	コマンド
ボリューム	エントリー ポイント	公開されたポート

[違反] セクションには、コンテナ イメージのルールを含む Kubernetes セキュリティ強化ポリシー ルールの違反数が表示されます。違反数は CVE コードの数と同じです。

[脆弱性のサマリ] セクションには、検出された脆弱性の円グラフが表示されます。任意のセクション（低、中、高、重大、不明）にカーソルを合わせると、そのカテゴリの脆弱性の数が表示されます。（これらの数値はチャートの下にも表示されます。）



[マルウェアとシークレットの検出] セクションには、疑わしいレピュテーションまたは悪意のあるレピュテーションを持つファイルと、シークレットを含むファイルが表示されます。

コンテナ イメージ スキャン レポートの表示 - レイヤー

コンテナ イメージ スキャン レポートのレイヤーを表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

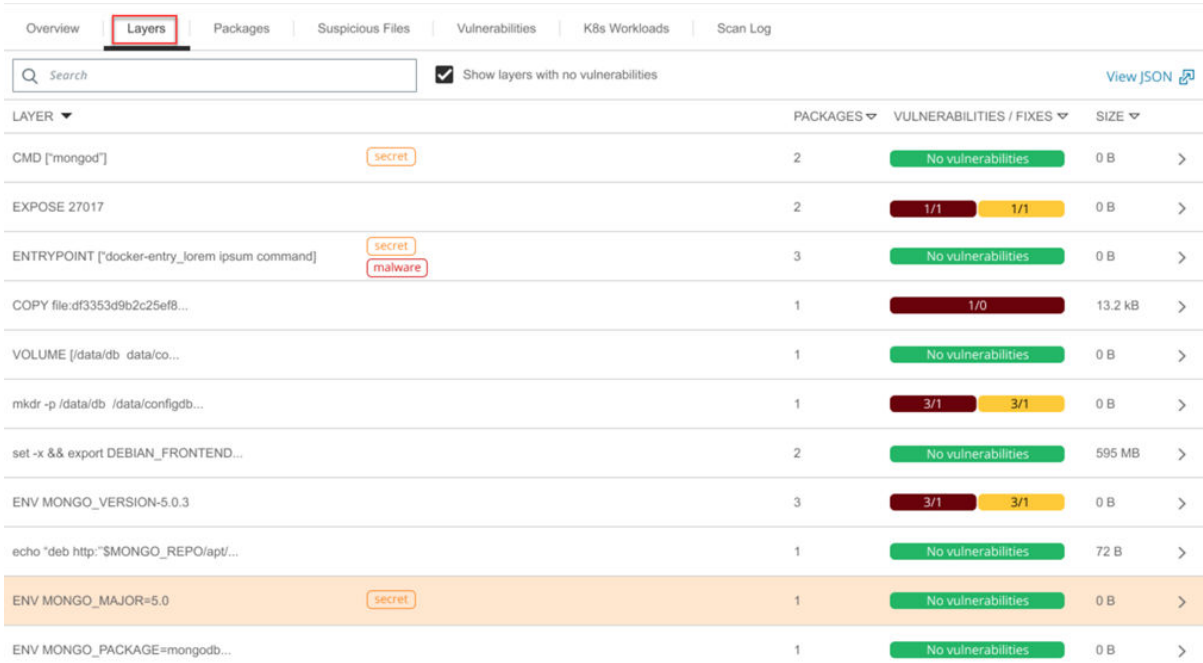
- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックします。

4 [レイヤー] タブをクリックします。

5 特定のレイヤーを検索できます。また、レイヤー テーブルの結果を脆弱性のあるレイヤーのみに制限することもできます。[脆弱性のないレイヤーを表示] チェック ボックスを選択解除します。



[レイヤー] タブには、次の情報が表示されます。

- レイヤー名
- `secret` または `malware` タグ(該当する場合)
- レイヤ内のパッケージ数
- 脆弱性と適用可能な修正
- レイヤー サイズ

6 レイヤーの詳細については、レイヤー行の右側にある矢印  アイコンをクリックします。

LAYER DETAILS

Layer ADD file:a5ec219cbfc4e0c31e7df48cc51abd9a5b92...
Layer digest sha256:ce8168f123378f7e04b085c9672717013d1d28b2aa726361bb132c...
Packages 114
Size 109 MB

MALWARE DETECTION

No malware found

VULNERABILITIES

CVE	PACKAGE	FIX	EXCEPTION
CVE-2021-202...	libgnutls30	Yes	No
CVE-2021-202...	libgnutlsxx28	Yes	No
CVE-2021-202...	libgnutls30	Yes	No
CVE-2021-202...	libgnutlsxx28	Yes	No
CVE-2021-335...	libc-bin	Yes	No

Show all (329)

SECRET DETECTION

No secrets found

PACKAGES

NAME	TYPE	VERSION
adduser	deb	3.118
apt	deb	1.8.2
base-files	deb	10.3+deb10u2

[レイヤーの詳細] パネルでは、次の操作を実行できます。

- [レイヤー] フィールドからイメージ レイヤーの作成に使用したコマンドをコピーします。

- [レイヤー ダイジェスト] フィールドにレイヤーの一意の識別子が表示を表示します。
- マルウェアを表示します。
- このレイヤーのすべての脆弱性を表示します。[脆弱性] セクションの[すべて表示] をクリックすると、[脆弱性] タブに移動します。コンテナ イメージ スキャン レポートの表示 - 脆弱性を参照してください。
- 脆弱性のサマリを表示します。CVE の左側にあるキャレット › アイコンをクリックします。

- シークレットを表示します。
- このレイヤーのすべてのパッケージを表示します。[パッケージ] セクションで [すべて表示] をクリックすると、[パッケージ] タブに移動します。コンテナ イメージ スキャン レポートの表示 - パッケージを参照してください。

コンテナ イメージ スキャン レポートの表示 - パッケージ

コンテナ イメージ スキャン レポート内のパッケージを表示するには、次の手順を実行します。

手順

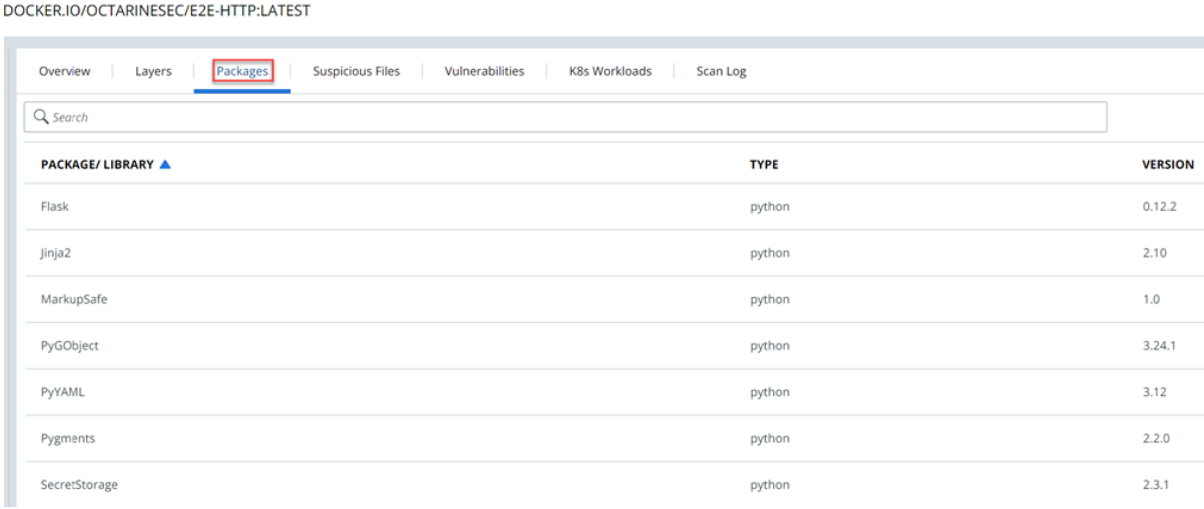
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [パッケージ] タブをクリックします。



[パッケージ] タブには、次の情報が表示されます。

- パッケージとライブラリ
- パッケージ タイプ
- パッケージ バージョン

表示されるパッケージのリストは、[タイプ] および [レイヤー] でフィルタリングできます。たとえば、`74fbdd4b6d6206a97532d4156e0` レイヤーを選択すると、検索結果にはそのレイヤーに属するパッケージのみが含まれます。

コンテナ イメージ スキャン レポートの表示 - 疑わしいファイル

コンテナ イメージ スキャン レポート内の疑わしいファイルを表示するには、次の手順を実行します。

手順

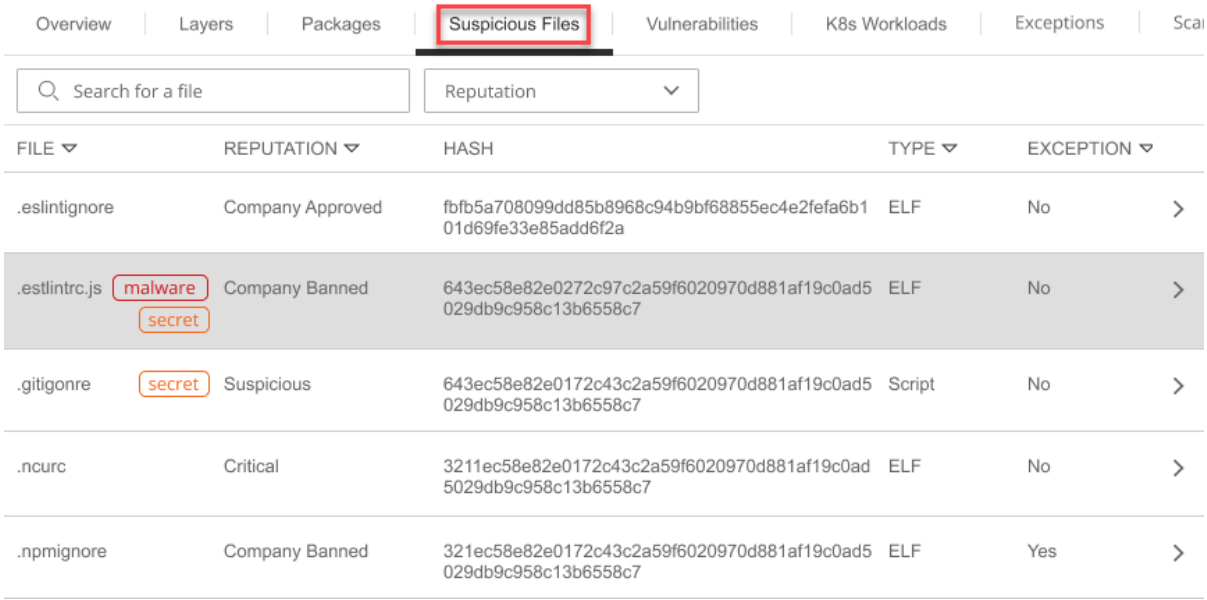
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

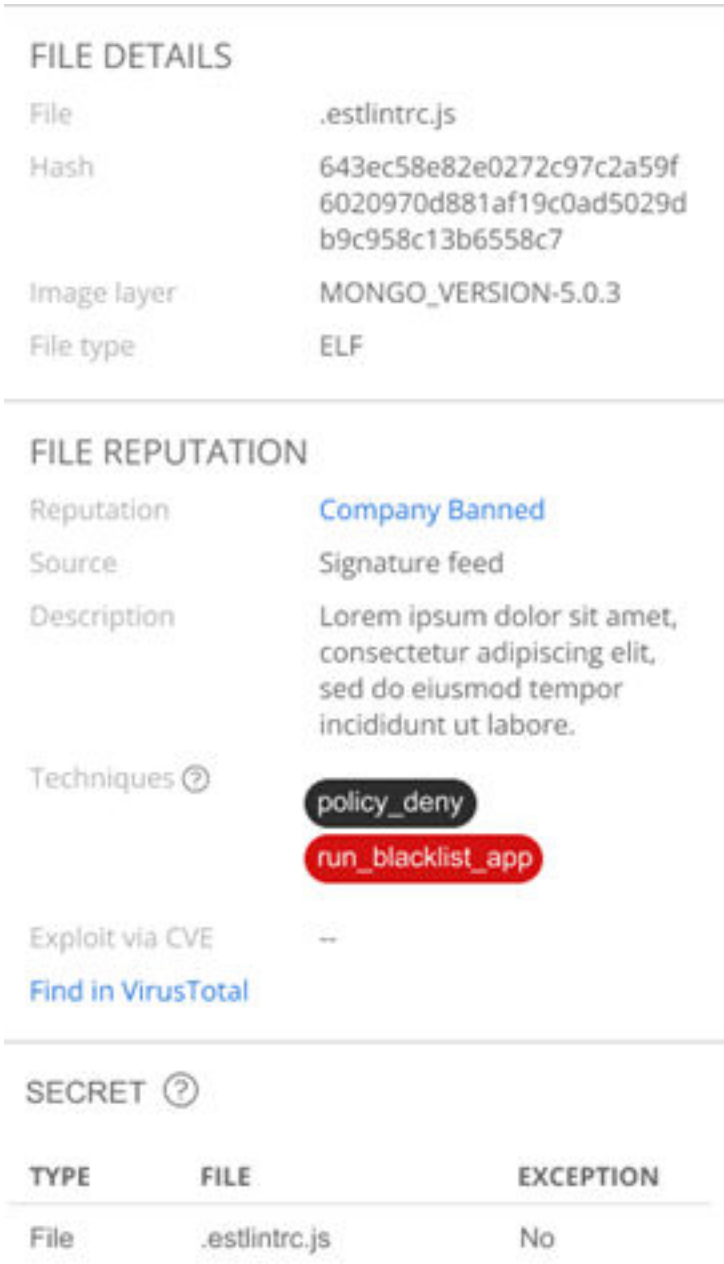
3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [疑わしいファイル] タブをクリックします。



表示されるファイルのリストは、[ファイル]、[レピュテーション]、[タイプ]、[例外] 別に並べ替えることができます。

5 ファイルの詳細については、行の右側にある矢印  アイコンをクリックします。



コンテナ イメージ スキャン レポートの表示 - 脆弱性

コンテナ イメージ スキャン レポートの脆弱性を表示するには、次の手順を実行します。

手順

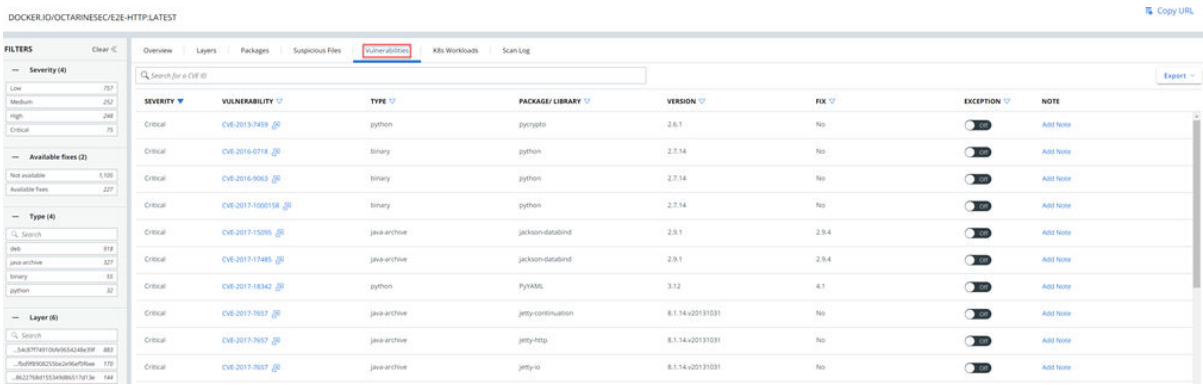
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

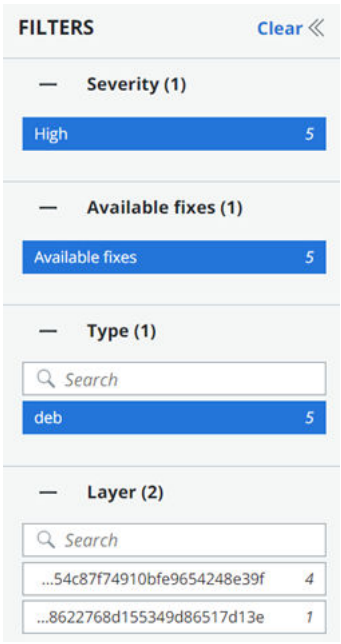
2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [脆弱性] タブをクリックします。



脆弱性のリストは、重要度、使用可能な修正、タイプ、およびレイヤーでフィルタリングできます。たとえば、重要度が高く、修正が使用可能で、`deb` タイプの脆弱性のみを表示できます。



5 検索を実行するか、すべての脆弱性を表示します。脆弱性の結果リストには、次のフィールドが含まれます。

- [重要度]コンテナ イメージには、それぞれ異なるリスク スコアを持つ複数の脆弱性が存在する可能性があります。このスコアに基づいて、脆弱性は重要度のレベル（クリティカル、高、中、低）でフィルタリングされます。重要度スコアリングを参照してください。
- [脆弱性]CVE タグをクリックすると、詳細が表示されます。コンテナ イメージ スキャン レポートの表示 - 脆弱性の詳細を参照してください。
- [タイプ]パッケージ タイプに基づいて脆弱性をフィルタリングできます。たとえば、`dpkg` パッケージは Debian Linux タイプです。
- [パッケージ/ライブラリ]
- [バージョン]
- [使用可能な修正]修正が可能な場合は、パッケージとバージョンを表示できます。
- [例外] の切り替え。脆弱性の例外を許可を参照してください。
- [メモ][メモを追加] をクリックしてこの脆弱性に関するメモを追加します。たとえば、除外を作成する場合は、除外の理由をメモすると便利です。

6 脆弱性データを CSV ファイルにエクスポートするには、[エクスポート] をクリックします。

コンテナ イメージ スキャン レポートの表示 - 脆弱性の詳細

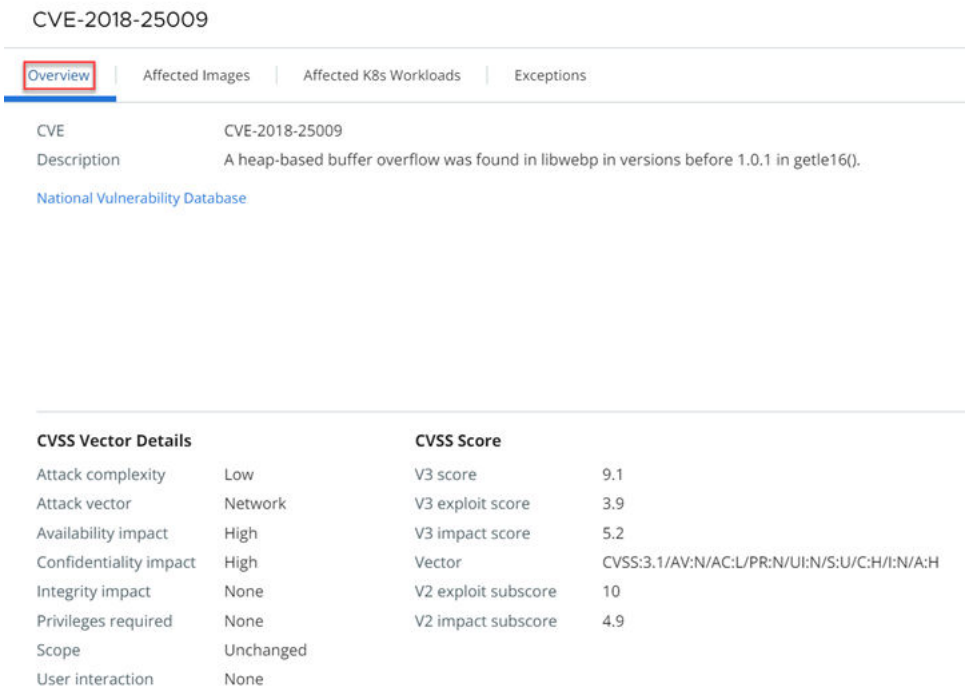
コンテナの脆弱性に関する詳細は、[コンテナの詳細] パネルで確認できます。

前提条件

コンテナ イメージ スキャン レポートの表示 - 脆弱性の手順 1 ～ 5 を実行します。

手順

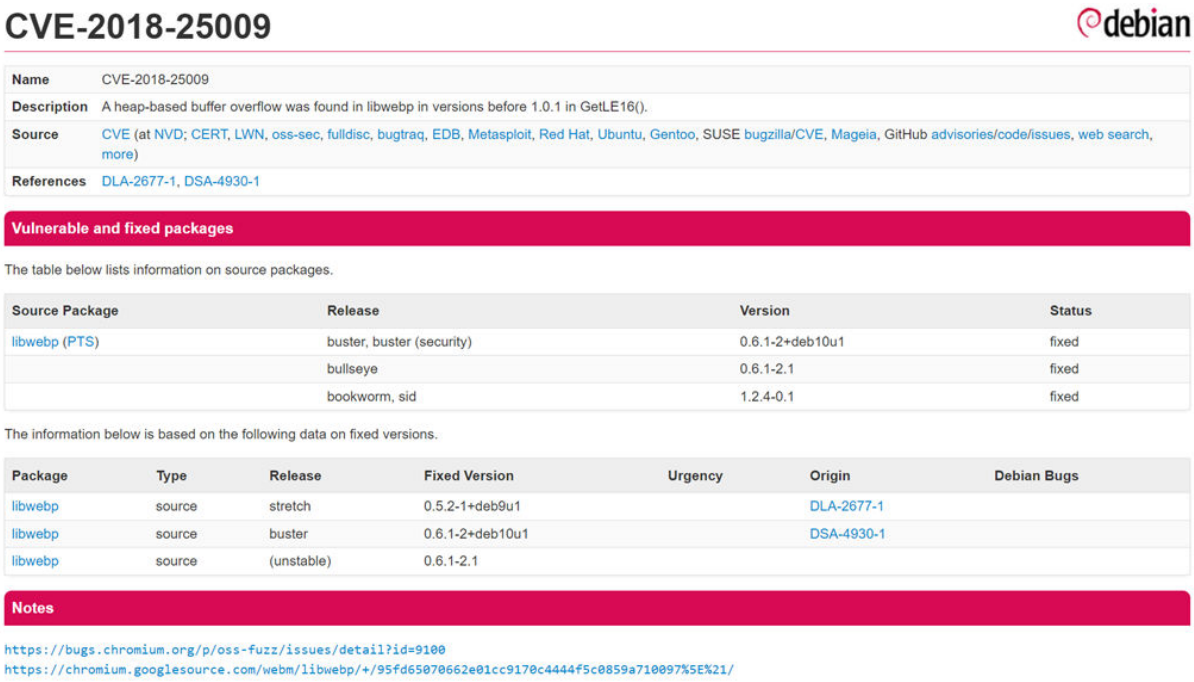
1 詳細を表示する脆弱性を選択します。[脆弱性] 列で CVE タグをクリックします。



デフォルトでは、[概要] タブが開きます。このタブには、次の詳細を表示できます。

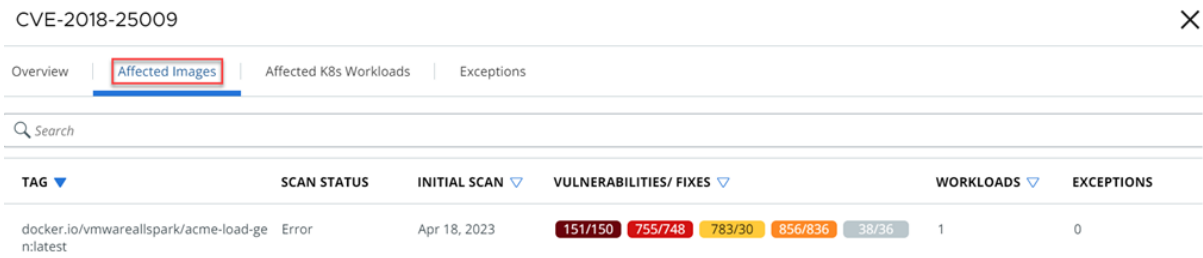
- [CVE] 識別子
- [説明]
- [CVSS ベクトル]
- [CVSS スコア]

外部 Web サイトで CVE の詳細を表示するには、[脆弱性情報データベース] をクリックします。例：

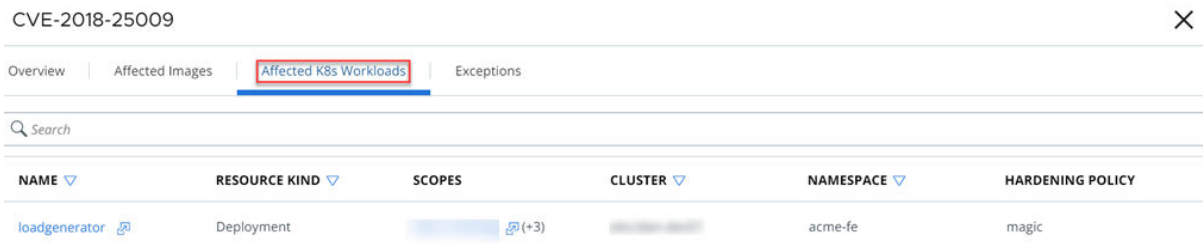


2 この脆弱性の影響を受けるイメージを表示するには、[影響を受けるイメージ] タブをクリックします。

次の情報が表示されます。



3 この脆弱性の影響を受ける Kubernetes ワークロードを表示するには、[影響を受ける K8s ワークロード] タブをクリックします。



[影響を受ける K8s ワークロード] タブでは、以下を実行できます。

- ワークロード名をクリックして、[Kubernetes ワークロード] パネルを開きます。Kubernetes ワークロードの表示 - 概要を参照してください。
- [範囲] をクリックして、関連付けられた範囲に関するサマリ情報を表示します。

4 脆弱性に例外がある場合は、[例外] タブに一覧表示されます。脆弱性の例外を許可を参照してください。

コンテナ イメージ スキャン レポートの表示 - K8s ワークロード

コンテナ イメージ スキャン レポートの Kubernetes ワークロードを表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [K8s ワークロード] タブをクリックします。

コンテナ イメージに関連付けられている Kubernetes ワークロードが一覧表示され、次のフィールドが含まれます。

- ワークロード[名]名前をクリックして、[ワークロードの詳細] パネルを開きます。Kubernetes ワークロードの監視を参照してください。
- DaemonSet などの [リソースの種類]
- [範囲]
- ワークロードを含む [クラスタ]
- [名前空間]
- [セキュリティ強化ポリシー]ポリシーの名前をクリックしてそのサマリを表示します。

コンテナ イメージ スキャン レポートの表示 - スキャン ログ

コンテナ イメージ スキャン レポートのスキャン ログを表示するには、次の手順を実行します。

手順

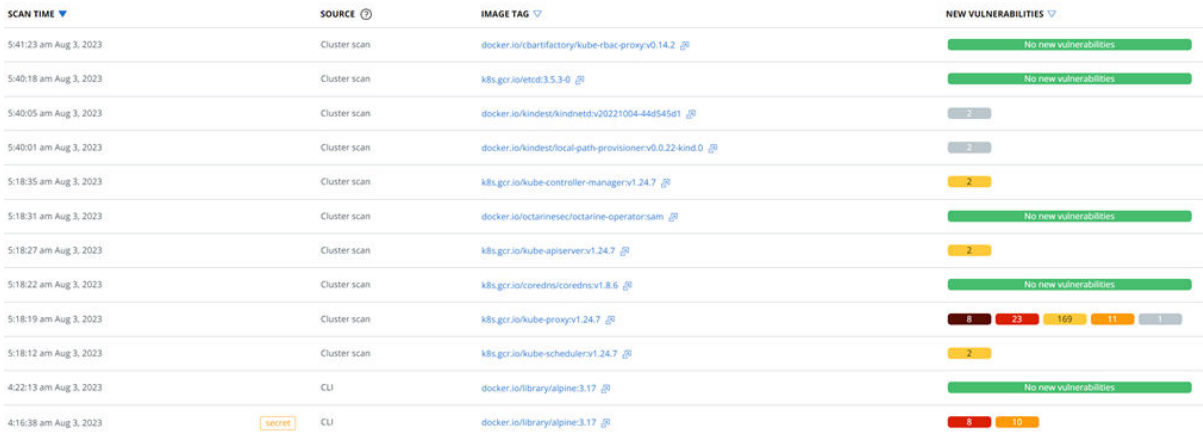
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [スキャン ログ] タブを選択します。



5 オプションで、スキャン ログのリストの時間枠を指定します。デフォルトの時間枠は [すべて利用可能] です。脆弱性の結果リストには、次のフィールドが含まれます。

- [スキャン時間]
- [送信元] — スキャンをトリガした原因
- [ワークロード]
- [新しい脆弱性]

コンテナ イメージの脆弱性の調査

コンテナ イメージは、脆弱性情報データベースの既知の脆弱性と照合されます。構成済みの Kubernetes ポリシーに基づいて、セキュリティの脆弱性を表示し、その脆弱性に対する修正の可用性を確認して、パッチや更新をスケジュール設定できます。

手順

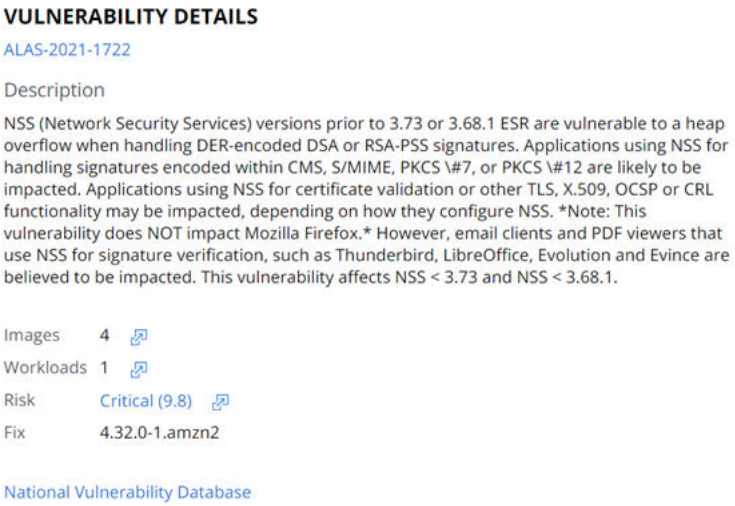
1 左側のナビゲーション ペインで、[セキュリティ強化] - [脆弱性] の順にクリックします。

2 [コンテナ イメージ] タブをクリックします。

デフォルトの重要度フィルタは [クリティカル] です。重要度に関係なくすべての脆弱性を表示するには、[すべて] をクリックします。

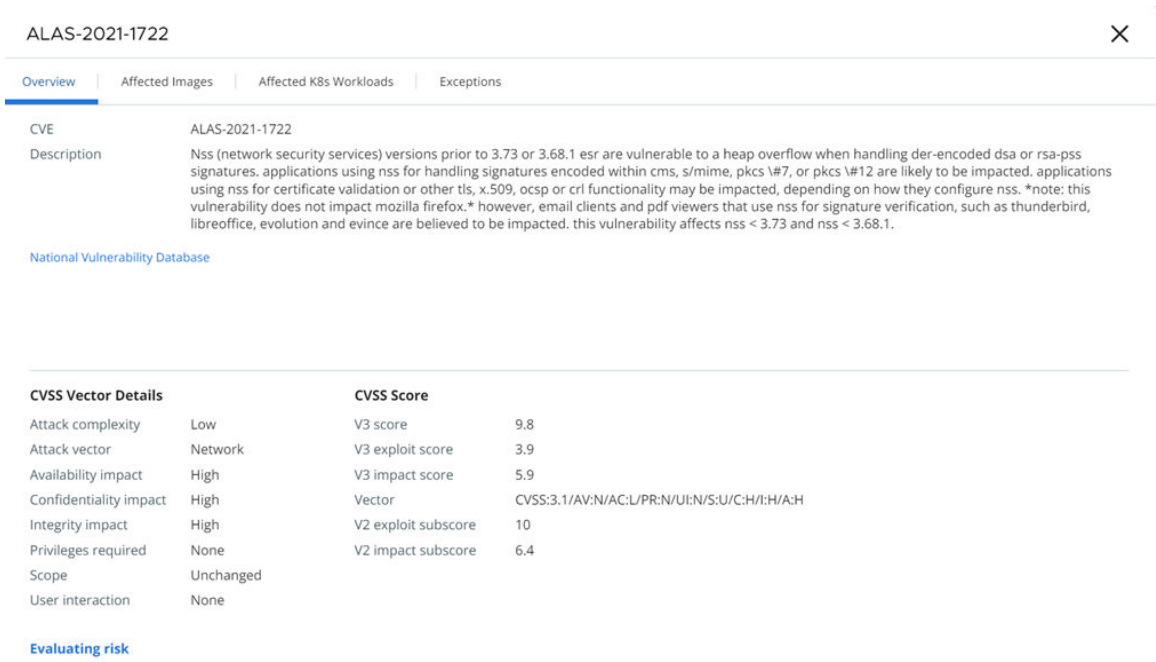
デフォルトでは、CLI クライアントを使用してスキャンされるすべてのコンテナ イメージの脆弱性を確認できます。Kubernetes 環境でのみ実行されている脆弱性をフィルタリングするには、右上の [Kubernetes で実行] チェックボックスをオンにします。

3 行をダブルクリックするか、行の右側にある矢印  アイコンをクリックして、[脆弱性の詳細] パネルを表示します。



このパネルでは以下を実行できます。

- [イメージ] の横にあるリンク アイコンをクリックして、[脆弱性] パネルの [影響を受けるイメージ] タブを開きます。
- [ワークロード] の横にあるリンク アイコンをクリックして、[脆弱性] パネルの [影響を受ける K8s ワークロード] タブを開きます。
- [リスク] カテゴリの横にあるリンク アイコンをクリックして、[脆弱性] パネルの [概要] タブを開きます。



- 脆弱性リファレンス タグまたは [脆弱性情報データベース] をクリックして、関連する外部の Web 画面を開きます。

コンテナ イメージ スキャン レポートの表示 - 脆弱性の詳細を参照してください。

脆弱性の例外を許可

イメージの脆弱性の例外を作成できます。例外は、Kubernetes セキュリティ強化ポリシーによってスキップされます。

イメージには多くの脆弱性がある可能性があります。それらの一部は環境にリスクを引き起こさないと考える場合は、特定のイメージに限りこれらの脆弱性の例外を有効にできます。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 [イメージ タグ] 列でイメージの名前をクリックして、[イメージ スキャン レポート] を開きます。

4 [脆弱性] タブをクリックします。

5 [例外] 列で、ON を切り替えて例外を有効にします。このイメージに対してこの脆弱性をキャプチャする Kubernetes セキュリティ強化ポリシーは、これ以上のアクションを制限しません。

6 [メモを追加] をクリックします（または、この脆弱性に関するメモがすでにある場合は、[編集]

アイコンをクリックして編集します）。除外の理由を入力し、[保存] をクリックします。これはオプションですが、推奨される手順です。

結果

コンテナ イメージ ルールを含む Kubernetes セキュリティ強化ポリシーのルール検証では、例外を含むイメージをスキップします。

コンテナ イメージでのファイル レピュテーションの管理と表示

レピュテーションは、アプリケーションに与えられた信頼度または不信頼度のレベルです。レピュテーションは、複数の情報源の既知の良いレピュテーションおよび悪いレピュテーションに基づいています。システム内のファイル レピュテーションを表示するには、さまざまな方法があります。

ファイルが疑わしい場合、または既知のマルウェアと一致する場合、ファイル レピュテーション サービスは、Carbon Black Cloud コンソールでそのようにラベル付けします。SHA-256 ハッシュを介して会社の禁止リストまたは承認リストに追加されたバイナリも検出され、悪意のあるまたは信頼できるとしてラベル付けされます。

重要： Carbon Black は、ブラックリストとホワイトリストという用語を禁止リストと承認リストに置き換えます。API、TTP、およびレピュテーションの用語の更新に先立って、通知が提供されます。

注：

- Carbon Black Cloud コンソールは、マルウェア バッジが malware の会社の禁止ファイルまたは重大なファイルがあるイメージを示します。

  マルウェア バッジは、Carbon Black Cloud がイメージ ファイルを部分的または完全に悪意があると見なした場合にのみ表示されます。たとえば、 会社の禁止リストに追加されたマルウェア ハッシュのマルウェア バッジが表示されます。会社のポリシーを通じてブロックされたハッシュのマルウェア バッジは表示されません。
- MD5 はサポートされていません。ハッシュは SHA-256 形式である必要があります。

コンテナ イメージ内のマルウェアの検出

クラスタ イメージ スキャンは、既知のファイルの広範なデータベースと比較することで、検出されたソフトウェアを特定して分類するのに役立ちます。

セキュリティ管理者は、イメージ スキャンのファイル レピュテーション機能を使用して、特定のコンテナ イメージのすべての Linux ELF ファイルを既知の悪意のあるファイルのリストに対して分析できます。

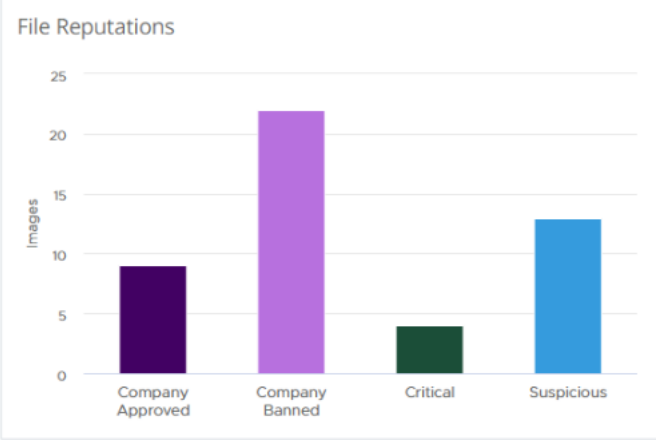
DevSecOps として、クラスタに展開されているすべてのコンテナ イメージの疑わしい/悪意のあるファイル レピュテーションを表示できます。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

[コンテナ イメージ] 画面には、Kubernetes 環境で現在何が発生しているかを示す一般的なサマリが含まれています。[ファイル レピュテーション] ウィジェットは展開されたコンテナ イメージのすべてのレピュテーションを棒グラフで要約します。



この可視化により、疑わしいファイルを使用して実行されているイメージの数と、レピュテーション別の分布が明らかになります。

- [会社承認] — SHA-256 ハッシュによって会社の承認リストに追加されたファイルであることを示します。
- [会社禁止] — SHA-256 ハッシュによって会社の禁止リストに追加されたファイルであることを示します。
- [重大] - ファイルが既知のマルウェアであることを示します。クラウド分析と脅威インテリジェンス フィードは、既知のマルウェアのレピュテーションを判断します。
- [疑わしい] - イメージ ファイルが疑わしいマルウェアであることを示します。クラウド分析と脅威インテリジェンス フィードは、疑わしいマルウェアのレピュテーションを判断します。分析では、ファイルが良好かマルウェアかを判断できません。

2 ファイル レピュテーションがコンテナ イメージ内のファイルに割り当てる信頼または不信のレベルをさらに調査するには：

- [展開されたイメージ] タブをクリックし、イメージ行の右側にある矢印アイコンをクリックします。

  [イメージの詳細] パネルの [ファイル レピュテーション] セクションには、コンテナ イメージ内のすべての関心のあるファイルとその割り当てられたレピュテーションが一覧表示されます。

- [展開されたイメージ] タブで、そのコンテナ イメージの [イメージ タグ] 列の下にあるリンクをクリックします。

  [ファイル レピュテーション] ウィジェットは、[コンテナ イメージ] 画面の [概要] タブに表示されます。イメージの疑わしいファイルと悪意のあるファイルの分布を円グラフで表示します。

- [コンテナ イメージ] 画面で、[レイヤー] タブをクリックし、レイヤー行をダブルクリックします。

  [ファイル レピュテーション] セクションでは、ファイル名とレピュテーションを表示できます。

コンテナ イメージ内のファイル レピュテーションのオーバーライド

コンテナ イメージで実行されている疑わしいファイルまたは重大な（悪意のある）ファイルがある場合、そのファイルをレピュテーションに関する会社の承認リストまたは禁止リストのいずれかに追加することで、クラウドのレピュテーションをオーバーライドできます。

注： マルウェア バッジ malware は、Carbon Black Cloud がイメージ ファイルを部分的または完全に悪意があると見なした場合にのみ表示されます。

[適用] - [レピュテーション] 画面を使用して、不審なファイルのハッシュを削除したり、会社の承認レピュテーションまたは禁止レピュテーションのリストに追加したりすることもできます。

MD5 はサポートされていません。ハッシュは SHA-256 形式である必要があります。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [展開されたイメージ] タブを選択します。

3 コンテナ イメージを見つけて、[イメージ タグ] 列にあるリンクをクリックします。

4 [コンテナ イメージ] 画面で、[疑わしいファイル] タブをクリックします。

展開されたコンテナ イメージ内の疑わしいファイルまたは悪意のあるファイルのみが表示されます。

5 目的のファイルをダブルクリックします。

ファイルに疑わしいレピュテーションまたは重大なレピュテーションがある場合は、会社の承認ハッシュまたは禁止ハッシュのリストに追加できます。

注： ファイルがコンテナ イメージとエンドポイント内で実行されている場合、ファイルのレピュテーションをオーバーライドすると、エンドポイントにも適用されます。

a [アクション] ドロップダウン メニューから、[ハッシュを承認リストに追加] または [ハッシュを禁止リストに追加] を選択します。

b オプション: コメントを入力します。

c [追加] をクリックします。

フィードを更新するまでに最大 10 分かかります。

ファイルに会社の承認レピュテーションまたは禁止レピュテーションがすでに割り当てられている場合、そのリストから削除するオプションがあります。

a [アクション] ドロップダウン メニューから、[リストからハッシュを削除] を選択します。

b オプション: コメントを入力します。

c [削除] をクリックします。

ハッシュを使用した疑わしいファイルの詳細については、VirusTotal サービスを使用してください。

a [ファイルの詳細] パネルで、[アクション] ドロップダウン メニューから [VirusTotal で検索] を選択します。

サービスの Web サイトにリダイレクトされます。

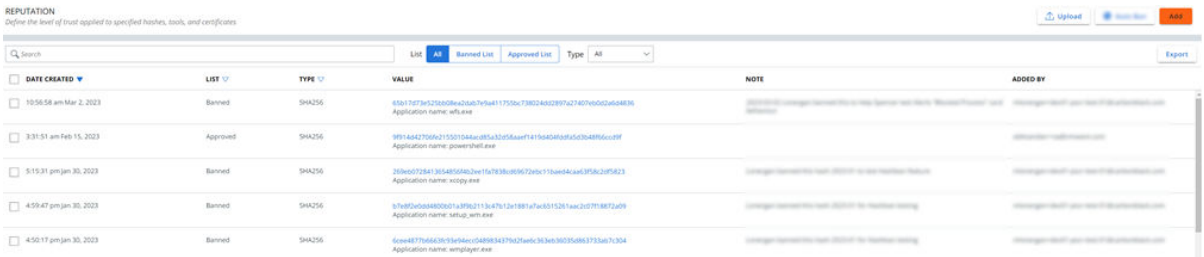
b 基本的な結果を確認し、それらを使用してシステムを改善します。

コンテナ イメージのファイル レピュテーションの管理

ファイル レピュテーションを管理する方法は複数あります。このトピックでは、 [適用] > [レピュテーション] 画面を使用してレピュテーション管理タスクを実行する方法について説明します。

手順

◆ 左側のナビゲーション ペインで、[適用] - [レピュテーション] の順にクリックします。



この画面では、次の操作を実行できます。

- リストを [すべて]、[ハッシュ]、[IT ツール] または [証明書] でフィルタリングします。
- ハッシュ、証明書、または IT ツールのリストを含む CSV ファイルをアップロードします。画面の右上にある [アップロード] ボタンをクリックし、画面上の指示に従います。
- レピュテーションをファイルに追加します。コンテナ イメージでのファイル レピュテーションの追加を参照してください。
- レピュテーション データを CSV ファイルにエクスポートします。ページの右上にある [エクスポート] ボタンをクリックします。
- ハッシュを削除します。ハッシュの左側にあるチェック ボックスを選択し、[削除] をクリックします。
- ファイルの発生を調査します。[値] 列のハッシュ値をクリックします。

コンテナ イメージでのファイル レピュテーションの追加

このトピックには、承認リストまたは禁止リストにレピュテーションを追加する概念的情報を記載しています。

パスでのワイルドカードの使用

パスを追加する際、ワイルドカードを使用して特定のファイルまたはディレクトリを対象にできます。

注： ワイルドカードを使用すると信頼済み認証局により署名されたように見える悪意のあるソフトウェアを偶発的に承認してしまう場合があるため、証明書を承認する場合はできるだけ具体的に行ってください。

ワイルドカード	説明	例
*	単一のサブディレクトリ レベルまでの 0 または連続文字に一致します。	`C:\program files*\custom application*.exe` `C:\program files\custom application\` または `C:\program files(x86)\custom application\` の実行ファイル
**	すべてのサブディレクトリ レベルの部分パスに一致し、繰り返されます。	`C:\Python27\Lib\site-packages**` そのディレクトリとそのすべてのサブディレクトリ内のファイル。
?	その位置にある 0 または 1 文字に一致します。	`C:\Program Files\Microsoft Visual Studio 1?.0**` MS Visual Studio バージョン 1 またはバージョン 10-19 のファイル。

ファイルの承認

承認リストへの追加は、指定されたアプリケーションの存在およびアクションを承認するものです。承認リストへの追加の効果はグローバルであり、アプリケーションの特定のバージョンに添付されているすべてのポリシーに適用されます。

次のような使用例で承認リストへの追加を使用します: ソフトウェア展開ツール、実行可能インストーラ、IDE、コンパイラ、スクリプト エディタなど。

Carbon Black では、承認されたアプリケーションを定期的に更新して、新しいバージョンに対応させることを推奨します。

[IT ツールおよび証明書を承認するメリット]

- IT ツールが即座に実行される新たな大量のコードをドロップした場合のパフォーマンスへの影響が最小限に抑えられます。
- IT ツールについては、新しいコードの実行により干渉されることはありません。ドロップされたコードはブロックされません。
- 証明書については、特定の証明書を使用して署名されたファイルの初回の実行がブロックされることはありません。
- 承認リストへの追加は、悪用を防止するための絶対的なものではありません。実行すると、新しいコードの遅延解析がバックグラウンドで始まります。

[承認された IT ツールおよび証明書に優先するレピュテーション]

- Company Black
- Company White
- 既知のマルウェア
- PUP マルウェア
- マルウェアの疑い
- Trusted White

ファイルの禁止

禁止リストへの追加は、指定されたアプリケーションの存在およびアクションを禁止するものです。禁止リスへの追加の効果はグローバルです。

禁止リストへのファイルの追加

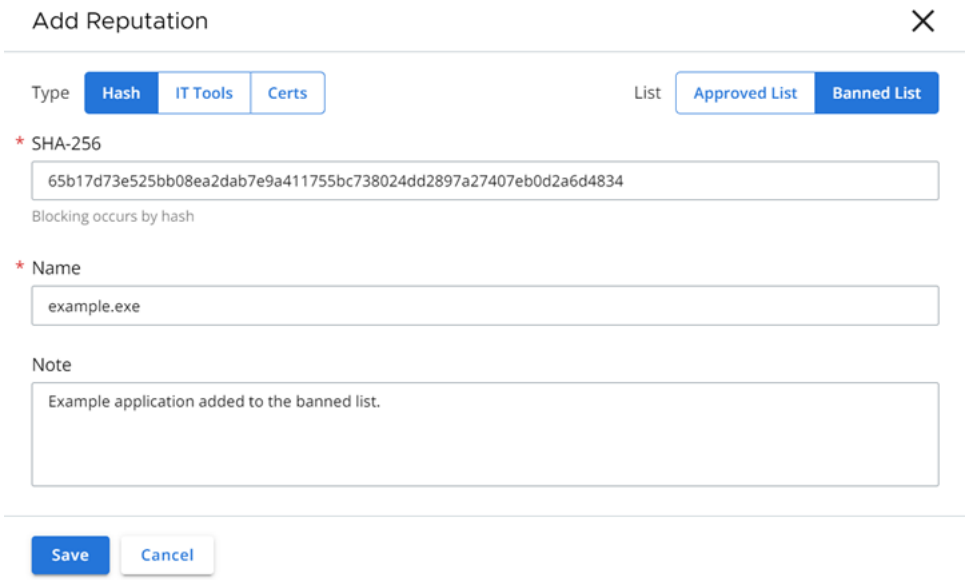
禁止リストにファイルを追加するには、次の手順を実行します。

注： MD5 はサポートされていません。ハッシュは SHA-256 形式である必要があります。

手順

1. 左側のナビゲーション ペインで、[適用] - [レピュテーション] の順にクリックします。
2. 画面の右上にある [追加] ボタンをクリックします。
3. タイプの [ハッシュ] をクリックします。
4. [禁止リスト] をクリックします。

5 ファイルの SHA-256 ハッシュ、ファイル名、およびファイルを禁止する理由を説明するメモを入力します。



6 [保存] をクリックします。

承認リストへのレピュテーションの追加

承認リストにファイル、信頼できる IT ツール、または証明書を追加するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [レピュテーション] の順にクリックします。

2 画面の右上にある [追加] ボタンをクリックします。

3 [承認リスト] をクリックします。

4 [タイプ] を選択します。

タイプ	入力するフィールド	メモ
[ハッシュ]	■ SHA-256 ハッシュ ■ ファイルの名前 ■ メモ (オプション)	MD5 はサポートされていません。ハッシュは SHA-256 形式である必要があります。 承認リストに追加されたハッシュは、レピュテーション階層で最も優先度が高い COMPANY_WHITE_LIST に割り当てられます。このステータスよりも他のレピュテーションが優先されることはありません。
[IT ツール]	■ 信頼できる IT ツールのパス ■ [すべての子プロセスを含める] の横にあるチェック ボックスをオンにして、このオプションを有効にします。 ■ メモ (オプション)	**ヒント:** パスにはワイルドカードを使用できます。パスでのワイルドカードの使用を参照してください。 選択した場合、新しく定義された信頼できる IT ツールの子プロセスによってドロップされたファイルも、初期信頼度を得ます。このオプションは、IT ツールが作業を委譲する子プロセスを作成し、その子プロセスがコピー コマンドのような一般的な実行ファイルを表す場合に役立ちます。 承認リストに追加されたアプリケーションに LOCAL_WHITE レピュテーションが割り当てられ、実行時に静的解析またはクラウド レピュテーションのために停止することはありません。
[証明書]	■ 証明書 (署名者) ■ 認証局の名前 ■ メモ (オプション)	この機能を使用するには、ファイルに署名し、有効な証明書で検証する必要があります。 承認リストに追加された証明書に LOCAL_WHITE レピュテーションが割り当てられ、実行時に静的解析またはクラウド レピュテーションのために停止することはありません。

5 [保存] をクリックします。

承認済み証明書の有効期限

すべての証明書には、証明書が有効と見なされる時間範囲を定義する有効範囲があります。

背景

ほとんどのデジタル署名ファイルには、コンテンツが改ざんされていないことを確認するコンテンツ署名と、ファイルがいつ署名されたかを確認するための別のカウンタ署名が含まれています。

これらのファイルでは、コード署名証明書の有効期限が切れている場合でも、コード署名証明書の有効範囲内で署名されたファイルは有効期限の観点から有効なままとなります。これは、カウンタ署名のタイムスタンプによって、証明書の有効期間中にファイルが署名されたことを確認できるためです。

まれにカウンタ署名/タイムスタンプが存在しないファイルでは、証明書の有効期限が切れると有効と見なされません。これは、証明書の有効期間中にファイルが署名されたかどうかを判断できなくなったためです。

証明書の失効は、有効期限とは別の概念です。失効は、以前に有効だった証明書が信頼できなくなったこと、有効期間の範囲が期限切れでなくても信頼すべきではないと示すために使用されます。

Carbon Black Cloud の期限切れの証明書の処理方法

Carbon Black Cloud は、Carbon Black Cloud がハッシュを初めて検出した場合にのみ、ファイル署名の有効性を確認します。この方法により、次のようなエッジ ケースが発生する可能性があります。

- タイムスタンプのないハッシュが証明書が有効なときにマシン 1 で検出され、有効期限が切れたときにマシン 2 で検出された場合、マシン 1 はファイルを証明書承認の対象として扱い続けます。マシン 2 は、ファイルを最初に無効/期限切れとして検出したため、ファイルを適格として扱いません。マシン 1 は最初に有効と見なしました。

  注： これはタイムスタンプ付きファイルには適用されません。これは、ファイルが有効範囲中に署名された場合に検証できるためです。

- 証明書が失効することが判明する前にハッシュが検出された場合、そのハッシュは承認され、後で取り消された証明書が見つかった場合でも、そのマシン上で承認されたままとなります。センサーが証明書が失効していることを認識した後に表示される、失効した証明書によって署名された新しいハッシュは、証明書の承認によって承認されませんが、他のレピュテーションによって承認される可能性があります。

要約すると、証明書の有効期限切れと失効は、システムに表示される新しいハッシュのレピュテーションに影響を与える可能性がありますが、アセット上にすでに存在するハッシュのハッシュレピュテーションには影響を与えません。センサーが証明書が失効していると判断した場合、または異なるセンサーに異なる信頼されたルート証明書ストアがある場合に、証明書の有効期限が切れているかどうか、カウンタ署名が存在しているかどうかに基づき、マシンに証明書承認ルールが異なるように適用される可能性があります。

シークレットの検出と防止

シークレットは、パスワード、トークン、キーなどの少量の秘密データを含むオブジェクトです。多くの場合、機密情報または外部サービスへのアクセスを制御するために、ユーザーまたはサービスを認証するために使用されます。シークレット管理は、ワークロード間でのシークレットの配布を制御および適用するのに役立つ不可欠なツールです。このセクションでは、Kubernetes 環境に展開されている静的に定義されたシークレットを検出して防止する方法について説明します。

Carbon Black Cloud シークレット管理は、ワークロードに挿入された静的シークレットを検出して防止するのに役立ちます。ポリシー ルールを使用して、シークレットを検出および防止できます。

注： シークレット検出はデフォルトでは無効になっています。クラスタを作成または編集する際に、この機能を有効にすることができます。クラスタの追加と Kubernetes センサーのインストールを参照してください。

シークレットに関するデータは、Carbon Black Cloud コンソールの次の画面で入手できます。

- コンテナ イメージの表示 - 概要
- 展開されたコンテナ イメージの詳細の表示
- [スキャンのログ] 画面でのコンテナ内のシークレットの検出
- コンテナ イメージ スキャン レポートの表示 - 疑わしいファイル

- コンテナ イメージ スキャン レポートの表示 - レイヤー
- コンテナ内のシークレットの防止

ロール

次のロールは、Carbon Black Cloud シークレット管理を使用できます。

[DevOps と DevSecOps]

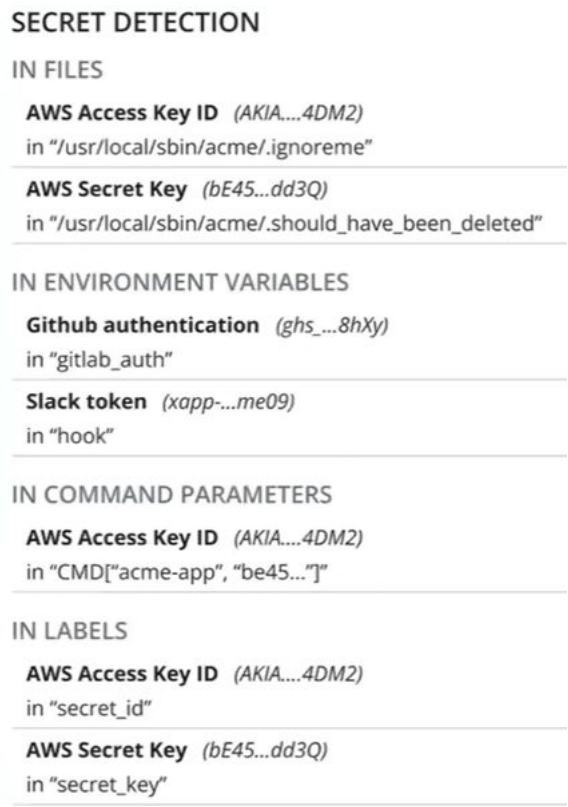
- イメージ ビルド フェーズでコンテナ内の静的に定義されたシークレットを検出して防止します。
- イメージ情報を検査して、潜在的なセキュリティ違反またはコンプライアンス違反の検出に役立ちます。
- ワークロード情報を検査して、潜在的なセキュリティ違反またはコンプライアンス違反の検出に役立ちます。
- ポリシーを使用して静的シークレットを持つイメージを使用するワークロードを拒否し、セキュリティとコンプライアンスを強化します。
- 静的シークレット ポリシー違反を確認して軽減します。
- 既存の調査にシークレットを含め、優先順位を付け、リスク プロセスを軽減します。
- 静的に定義されたシークレットを含むファイルを検出します。
- 展開されたすべてのイメージのシークレットをスキャンします。

[DevOps と開発者]

- イメージ情報を検査して、潜在的なセキュリティ違反またはコンプライアンス違反の検出に役立ちます。
- 静的シークレット ポリシー違反を確認して軽減します。

シークレット検出

シークレットは次の方法で検出されます。



データ タイプ

次の表に、キャプチャされたシークレット データ タイプの例を示します。

表 5-1. キャプチャされたシークレット データの例

ソース	カテゴリ	シークレット タイプ	秘密鍵	シークレット値
/.aws	ファイル	キーワード ディテクタ	aws_access_key_id	JKSN...3E3Q
`RUN /bin/sh -c echo hi --password "pddj...f837" # buildkit`	コマンド	キーワード ディテクタ	パスワード	pdhj...f837
azure	ラベル	Azure ストレージ アカウントのアクセス キー	azure	abcd...uv==
GITHUB_KEY	ENVIRONMENT_VARIABLE	Github 認証	GITHUB_KEY	ghu_...UKpr

シークレット タイプ

次の表に、Carbon Black Cloud が検出するシークレットのタイプを示します。

Azure ストレージ アカウントのアクセス キー	JFrog Artifactory 認証情報	AWS クライアント ID
AWS シークレット キー	Amazon Marketplace Web Service (MWS) キー	HTTP Bearer 認証
パスワードを含む URL	Github 認証	JSON Web トークン
Mailchimp API キー	npm 認証トークン	プライベート キー
Sendgrid API キー	Slack トークン	Square 認証
Stripe API キー	Twilio 認証	

[スキャンのログ] 画面でのコンテナ内のシークレットの検出

[イメージ スキャン レポート]の [スキャンのログ] 画面でコンテナ内のシークレットを検出するには、次の手順を実行します。

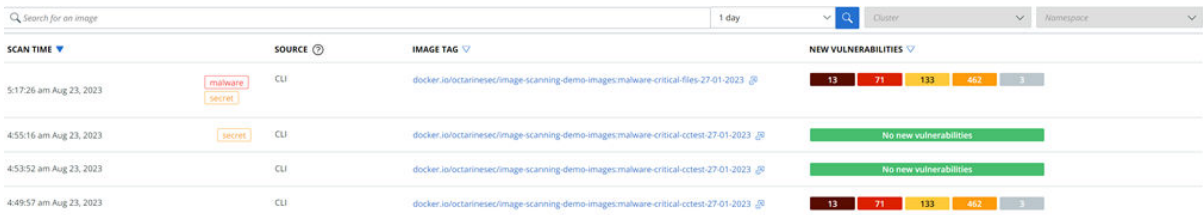
注： このトピックは、コンテナ内のシークレットを表示する 1 つの方法の例として提供されます。シークレット データを表示する Carbon Black Cloud コンソールの代替画面のリストについては、「シークレットの検出と防止」を参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

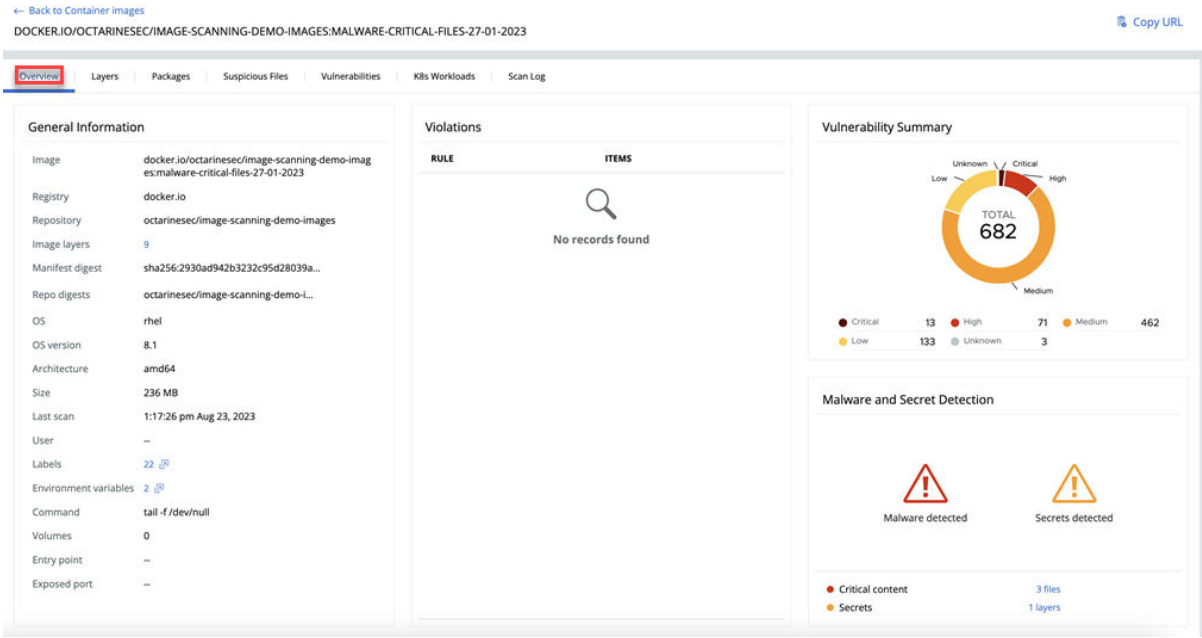
- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

2 [スキャン ログ] タブを選択します。



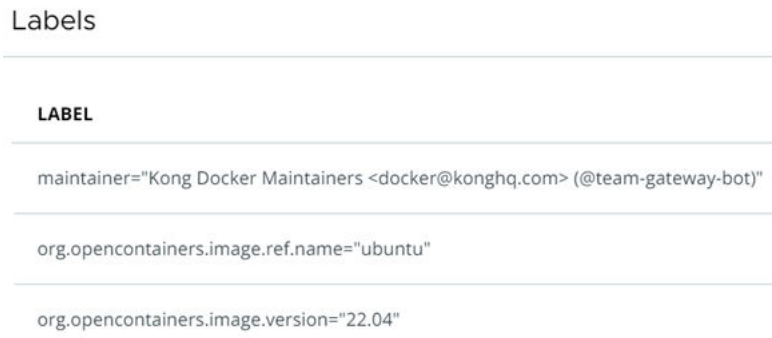
3 シークレットを含むイメージについては、[イメージ タグ] アイコンをクリックします。

このアクションにより、[イメージ スキャン レポート] の [概要] タブが開きます。



4 シークレットに関する追加情報は、次の方法で表示できます。

- [ラベル] アイコンをクリックします。例：



- [環境変数] アイコンをクリックします。例：

コンテナ内のシークレットの防止

コンテナ内のシークレットを防止するポリシー ルールを設定します。

手順

1 左側のナビゲーション ペインで、[適用] - [K8s ポリシー] の順にクリックします。

2 [セキュリティ強化ポリシー] タブをクリックします。

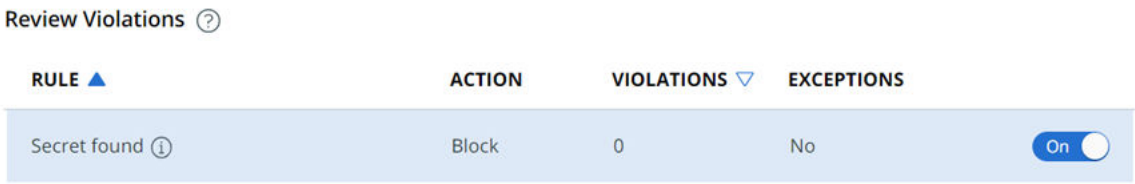
3 シークレット防止ルールを追加するポリシーを選択または作成します。

既存のポリシーを編集するには、「Kubernetes セキュリティ強化ポリシーの編集」を参照してください。新しいポリシーを範囲を作成するには、「Kubernetes セキュリティ強化ポリシーの作成」を参照してください。

4 [使用可能なルール] 画面で、[コンテナ イメージ] カテゴリの [シークレットの検出] ルールまで下にスクロールします。このルールは、シークレットを持つイメージの展開を防止します。[アラート] または [ブロック] を選択し、ルールの右側にある矢印  アイコンをクリックします。

ルールがポリシーに追加されます。

5 [次へ] をクリックします。



6 [次へ] をクリックします。

7 新しいポリシーを作成する場合は、[ポリシーを有効にする] または [ドラフトとして保存] をクリックします。既存のポリシーを編集する場合は、[保存] をクリックします。

Kubernetes ワークロードの監視

Carbon Black Cloud コンソールで、Kubernetes ワークロードのリスクの影響度と関連情報を確認できます。

Kubernetes 環境のワークロード レベルでリスクを修正し、問題を修正するため、以下を確認できます。

- リスクの重要度の詳細
- 適用された Kubernetes セキュリティ強化ポリシーとランタイム ポリシーの詳細
- Kubernetes セキュリティ強化ポリシーのポリシー違反
- Kubernetes ランタイム ポリシーのアラート

- 入力方向または出力方向トラフィックへのネットワーク接続

注：

- リスクの重要度に関する詳細については、Kubernetes リスクの重要度スコアリングを参照してください。
- ワークロードに関連するアラートの調査の詳細については、Kubernetes アラートのトリアージを参照してください。

Kubernetes ワークロードの表示

Kubernetes ワークロードを表示および評価するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

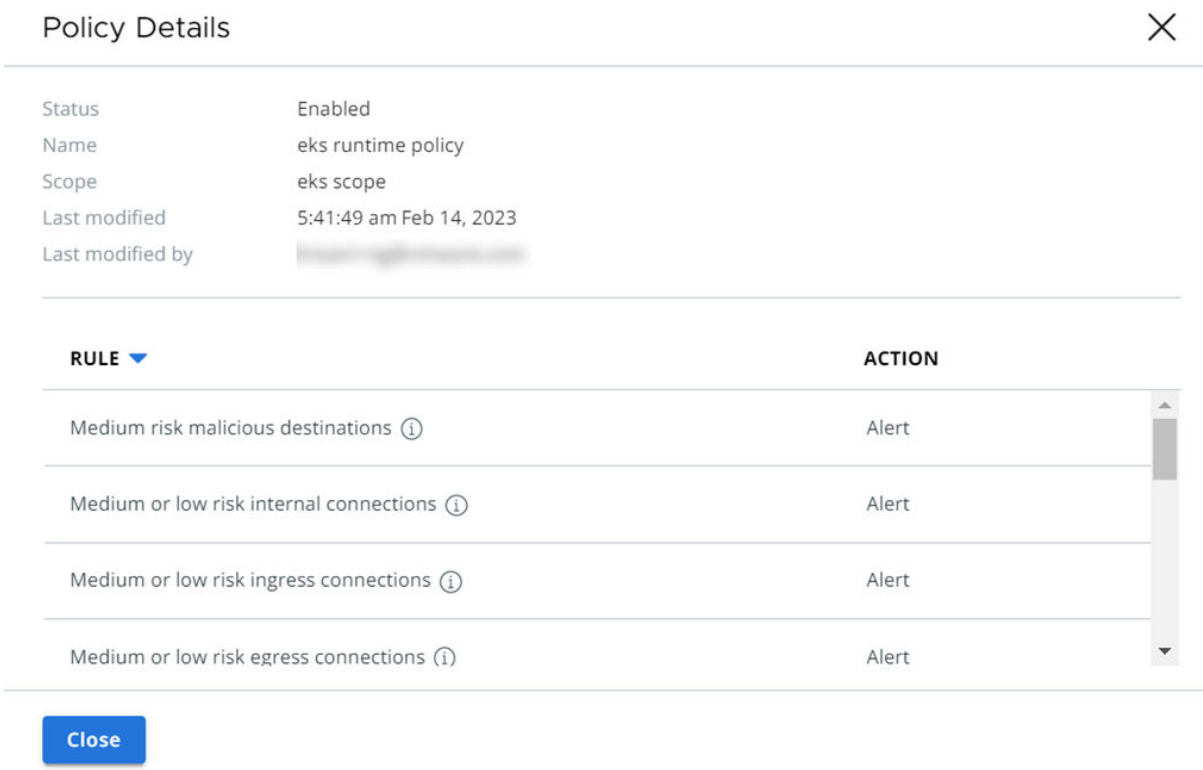
[Kubernetes ワークロード] 画面が開きます。

注： ルール適用事前設定を使用して値を適用してワークロードを変更した場合、そのワークロードは名前の横に**変更済み**ラベルが付いて表示されます。セキュリティ強化ルールの変更およびルールの結果の変更を参照してください。

残りの手順では、この画面のオプションについて説明します。

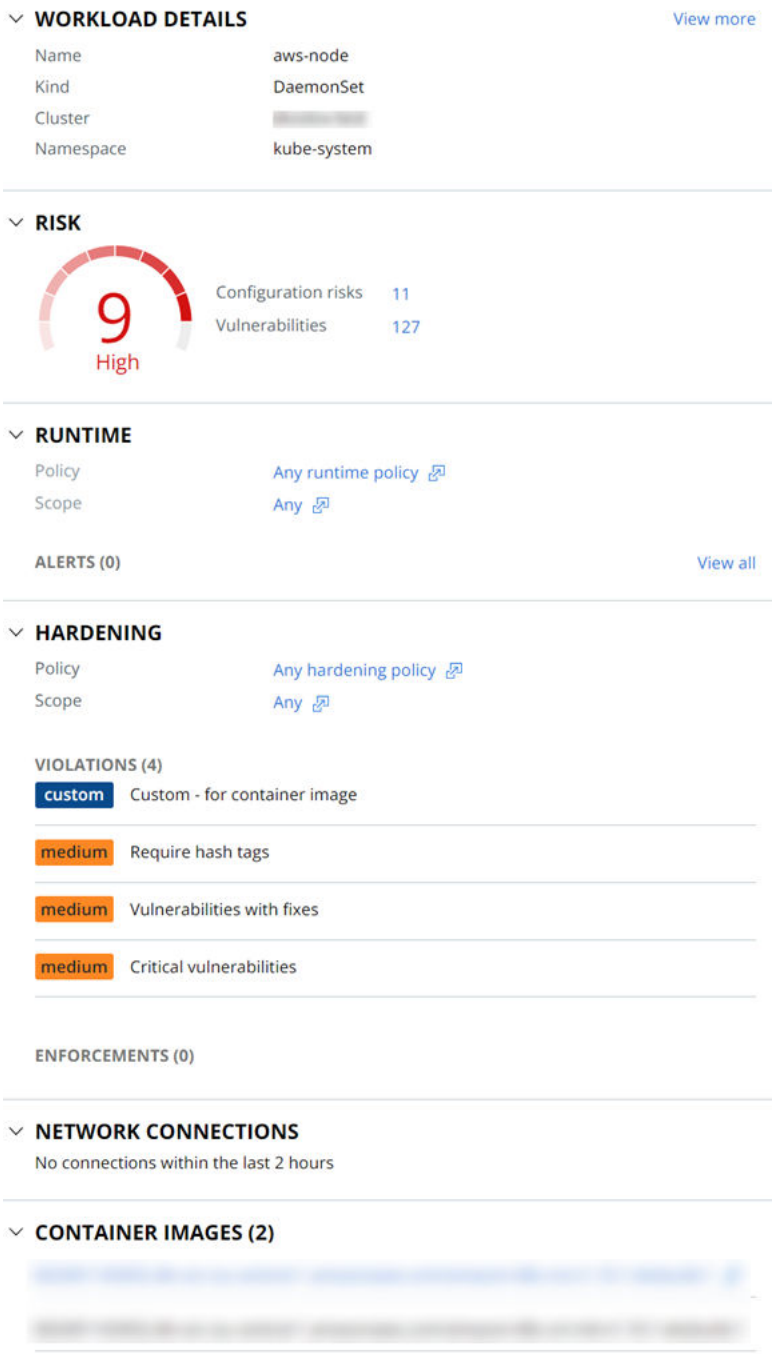
2 特定のワークロード画面を表示 - ワークロード名をクリックします。Kubernetes ワークロードの表示 - 概要を参照してください。

3 ワークロードに割り当てられているランタイム ポリシーを表示 - ランタイム ポリシー名をクリックします。[ポリシーの詳細] パネルには、ランタイム ポリシーのサマリが表示されます。



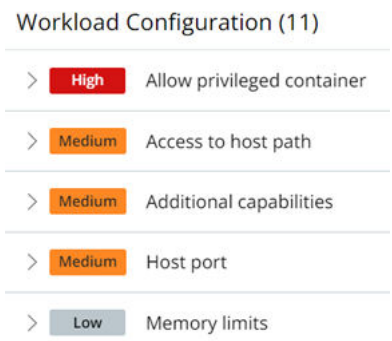
4 ワークロードに割り当てられているセキュリティ強化ポリシーを表示 - セキュリティ強化ポリシー名をクリックします。[ポリシーの詳細] パネルには、セキュリティ強化ポリシーのサマリが表示されます。

5 ワークロードの詳細を表示 - 行の右側にある 矢印  アイコンをクリックします。

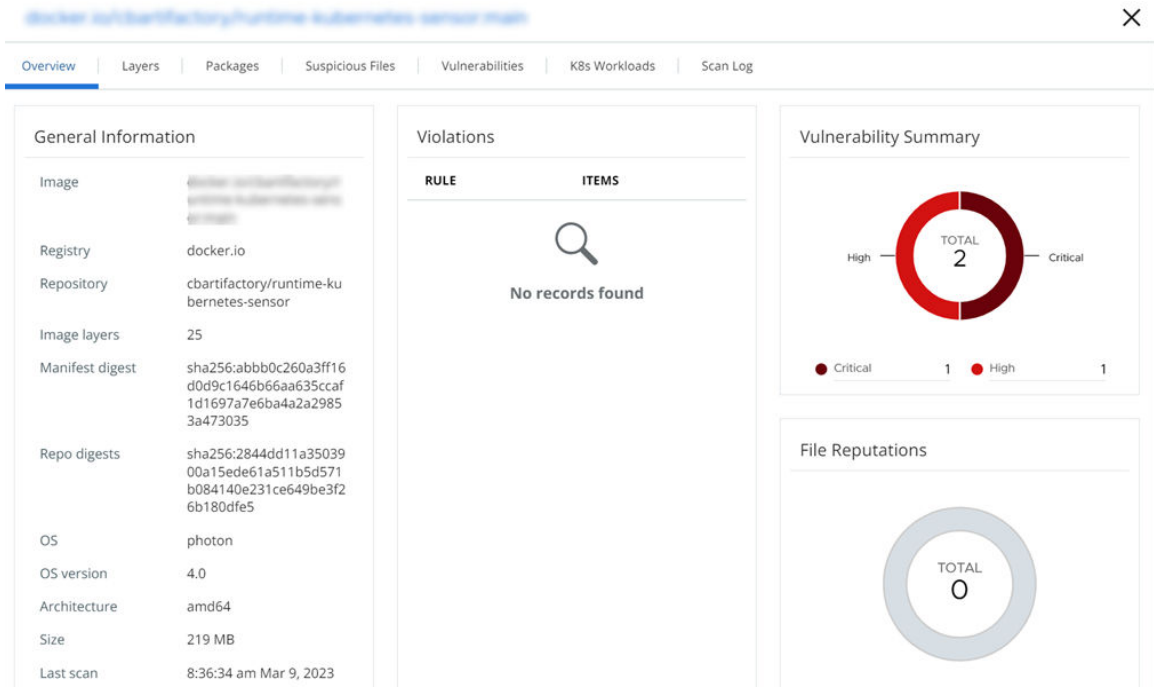


[ワークロードの詳細] パネルで、以下を表示できます。

- 特定のワークロード画面を表示 - [ワークロードの詳細] セクションで [詳細を表示] をクリックします。Kubernetes ワークロードの表示 - 概要を参照してください。
- ワークロードの構成リスクを重要度順に表示 - [リスク] セクションの [構成リスク] の横にある数をクリックします。



- ワークロードの脆弱性を重要度順に表示 - [リスク] セクションの [脆弱性] の横にある数をクリックします。
- ランタイム ポリシー、セキュリティ強化ポリシー、およびいずれかのポリシーに関連付けられる範囲は、[ランタイム] セクションと [セキュリティ強化] セクションでポリシーまたは範囲の名前をクリックして表示されます。
- ポリシー違反によって発生したアラートの数。このようなアラートをすべて表示するには、[ランタイム] セクションで [すべて表示] をクリックします。[アラート] 画面が開き、関連するアラートが一覧表示されます。Kubernetes アラートのトリアージを参照してください。
- セキュリティ強化ポリシーの違反と適用のリスト。
- 過去 2 時間以内のネットワーク接続。
- このワークロード内のコンテナ イメージ。ハイパーリンクされたコンテナ イメージ名をクリックすると、そのコンテナ イメージに関する情報を表示できます。



Kubernetes ワークロードの表示 - 概要

Kubernetes ワークロードの概要を表示するには、次の手順を実行します。

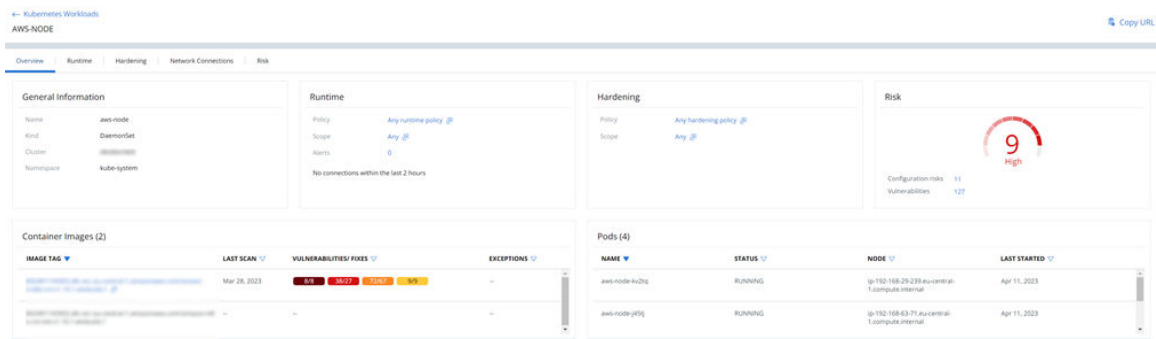
手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

2 2 番目の列でワークロードの名前をクリックします。

- [概要] タブには、次の詳細が表示されます。



- [一般情報] — 名前、種類、クラスタ、名前空間。

- [ランタイム] — 割り当てられたランタイム ポリシーおよび範囲。ポリシーまたは範囲名をクリックして、詳細を確認できます。このセクションには、ランタイム ポリシーに関連付けられているアラートが一覧表示され、過去 2 時間以内のネットワーク接続が表示されます。
- [セキュリティ強化] — 割り当てられたセキュリティ強化ポリシーと範囲。ポリシーまたは範囲名をクリックして、詳細を確認できます。
- [リスク] — このセクションでは、全体的なリスクの重要度、構成のリスク、および脆弱性を示します。詳細について [リスク] タブに移動するには、[構成リスク] または [脆弱性] の横にある数字をクリックします。Kubernetes ワークロードの表示 - リスクを参照してください。
- [コンテナ イメージ] — ワークロード内のコンテナ イメージを一覧表示します。ハイパーリンクされたコンテナ名をクリックすると、[コンテナ イメージ] 画面に移動できます。コンテナ イメージの表示 - 概要を参照してください。
- [ポッド] — 関連付けられたポッドのポッド名、ステータス、ノード、および最終開始日を一覧表示します。

Kubernetes ワークロードの表示 - ランタイム ポリシー

Kubernetes ワークロードのランタイム ポリシーの詳細については、次の手順を実行します。

Kubernetes ランタイム ポリシー も参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

2 2 番目の列で、ハイパーリンクされたワークロードの名前をクリックします。

3 [ランタイム ポリシー] タブをクリックします。

[ランタイム] タブには、このワークロードの次のランタイム ポリシー情報が表示されます。

- 名前
- 範囲
- アラート
- ワークロードのベースライン

  [ワークロードのベースライン] セクションには、次のデータが含まれています。

  - リモート接続
  - プロトコル
  - ポート
  - 接続タイプ

- ベースラインの動作を追加したユーザー
- アクション

ベースラインをリセットするには、[リセット] をクリックします。ランタイム ポリシーの Kubernetes 範囲ベースラインを参照してください。

Kubernetes ワークロードの表示 - セキュリティ強化ポリシー

Kubernetes ワークロードのセキュリティ強化ポリシーの詳細については、次の手順を実行します。

Kubernetes セキュリティ強化ポリシー も参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

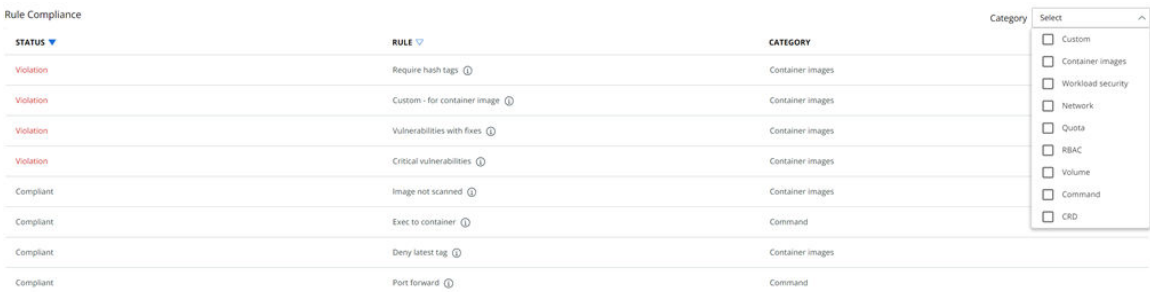
- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

2 2 番目の列で、ハイパーリンクされたワークロードの名前をクリックします。

3 [セキュリティ強化] タブをクリックします。

[セキュリティ強化] タブには、このワークロードに関する次のセキュリティ強化ポリシー情報が表示されます。

- 名前
- 範囲
- ルールの遵守



[ルールの遵守] セクションで、特定のカテゴリを選択して表示したり、すべてのカテゴリを表示したりできます。

Kubernetes ワークロードの表示 - ネットワーク接続

Kubernetes ワークロードに関連するネットワーク接続情報については、次の手順を実行します。

「ネットワーク アクティビティの分析」と「出力グループ」も参照してください。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

2 2 番目の列で、ハイパーリンクされたワークロードの名前をクリックします。

3 [ネットワーク接続] タブをクリックします。

接続のリストは、次の方法でフィルタリングできます。

- 出力方向
- 入力方向
- 内部
- アウトバウンド クロスネームスペース
- インバウンド クロスネームスペース

[パブリックの宛先]、[プライベートの宛先]、またはその両方を表示するかどうかを指定することもできます。

選択した接続の次のフィールドが表示されます。

- 接続先
- 出力グループ
- ポート
- プロトコル

Kubernetes ワークロードの表示 - リスク

Kubernetes ワークロードに関連するリスクを確認するには、次の手順を実行します。

「Kubernetes リスクの重要度スコアリング」と「コンテナ イメージの脆弱性の調査」も参照してください。

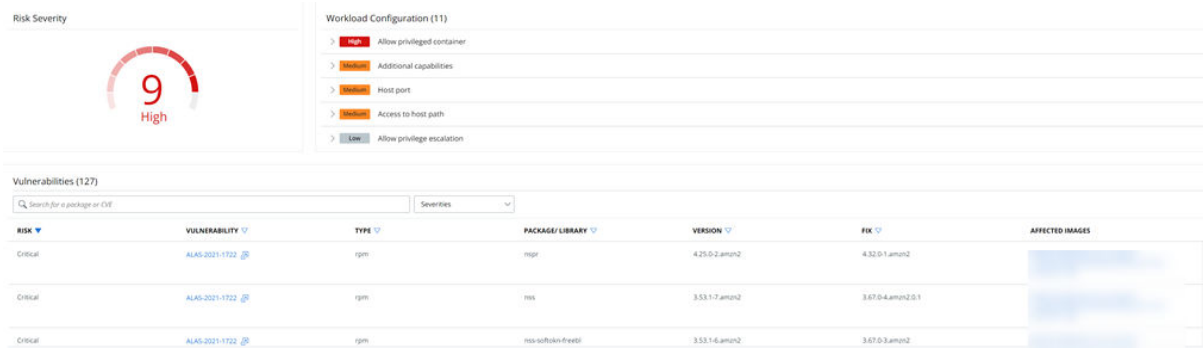
手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

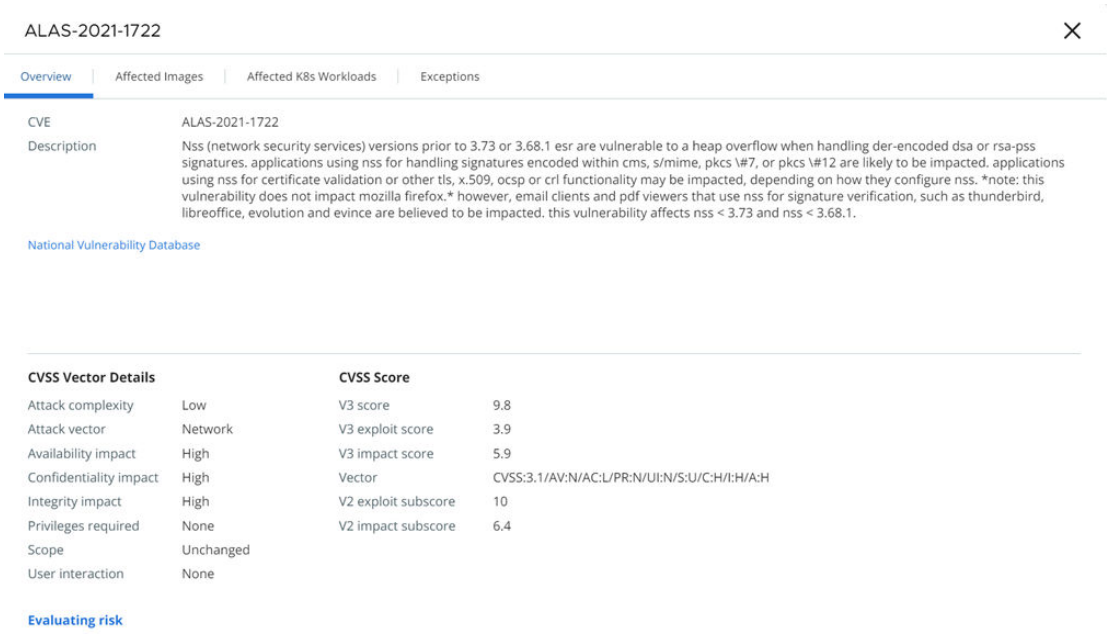
2 2 番目の列で、ハイパーリンクされたワークロードの名前をクリックします。

3 [リスク] タブをクリックします。



次のセクションでは、リスク評価と関連情報を提供します。

- [リスクの重要度] — このワークロードに関連付けられるリスクの重要度をまとめたものです。
- [ワークロード構成] — ワークロード構成のリスクをリスクの重要度順に一覧表示します。
- [脆弱性] — このワークロードの脆弱性に関する次の詳細を一覧表示します。表に表示する特定のパッケージまたは CVE を検索し、重要度でリストをフィルタリングできます。
  - リスクの重要度
  - 脆弱性名。このハイパーリンクをクリックすると、脆弱性の概要が表示されます。このパネルでは、影響を受けるすべてのイメージ、ワークロード、例外を表示できます。



  - タイプ
  - パッケージまたはライブラリ
  - 修正 (可能な場合)
  - 影響を受けるイメージ任意のイメージ名をクリックして、関連するコンテナ イメージ画面を開きます。

Kubernetes ワークロードの表示 - 動作モデル

Kubernetes ワークロードの動作モデルを表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ワークロード] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ワークロード] の順にクリックします。

2 2 番目の列で、ハイパーリンクされたワークロードの名前をクリックします。

3 [動作モデル] をクリックします。

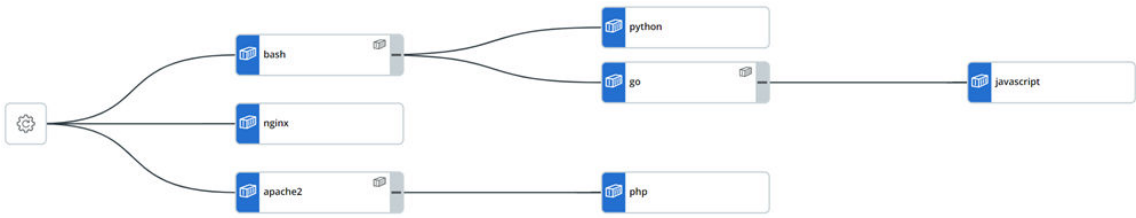
[動作モデル] 画面には、[ネットワーク モデル]、[プロセス アクティビティ モデル]、[ファイル アクセス モデル]、[リソース使用モデル] の 4 つのタブがあります。

- [ネットワーク モデル]

  このタブには、送信のプロセス名、トラフィック方向、リモート ホスト、リモート グループ、ポート、およびプロトコルが表示されます。

- [プロセス アクティビティ モデル]

  このタブにはプロセス ツリーが表示されます。例：



- [ファイル アクセス モデル]

  プロセス、ファイル、およびアクセス タイプが表示されます。

- [リソース使用モデル]

Kubernetes 仮想ワークロード

Kubernetes は、ユーザーに代わって一連のポッドを管理するワークロード リソースを提供します。これらのリソースは、目的のクラスタの状態に合わせて適切な数と種類のポッドを実行するようにコントローラを構成します。

一部のアプリケーションは、Kubernetes のワークロード コントローラを使用しません。これらは Carbon Black Cloud バックエンドに過負荷をかけ、それ以外の場合は非表示の大量のオブジェクトを使用してユーザー エクスペリエンスを強化します。クラスタの目的の状態を管理するため、Carbon Black Cloud はネイティブの Kubernetes コントローラを介して生成されないポッドをグループ化して、仮想ワークロード ロジックを自動的に適用します。仮想ワークロードは、任意のネイティブ ワークロードのように動作します。システム内に仮想ワークロードがある場合は、名前の [インベントリ] - [Kubernetes] - [ワークロード] 画面で  アイコンをクリックすると、そのラベルが付けられます。

ネットワーク アクティビティの分析

Carbon Black Cloud コンソールで、Kubernetes クラスタのネットワーク アクティビティを表示して分析できます。ネットワーク マップは、クラスタ内で実行されているすべての名前空間とワークロードとそのネットワーク トラフィックをグラフィック表示したものです。

ネットワーク マップは、ワークロードおよびネットワーク アクティビティから発生したアラートを特定するのに役立ちます。これらはマップ上で強調表示され、簡単に使用できます。ネットワーク マップには、クラスタの入力方向と出力方向の接続の概要が表示され、個々の名前空間とワークロードに焦点が絞られます。マップでは、名前空間、ワークロード、入力または出力グループを選択でき、ワークロードのネットワーク セキュリティ違反を含むトラフィックと関連する詳細が表示されます。マップは、過去 24 時間に収集されたデータに重点を置いています。

注： ワークロードの表形式のネットワーク データを表示したり、ネットワーク マップでこのアクティビティを表示したりできます。Kubernetes ワークロードの表示 - ネットワーク接続を参照してください。

Carbon Black Cloud コンソールでは、Kubernetes ワークロードが NodePort サービスまたはロード バランサ サービスの入力方向タイプを介してインターネットに公開される方法を確認できます。入力方向の詳細については、入力方向（外部リンク）を参照してください。

出力方向トラフィックはクラスタから別のネットワーク（パブリックまたはプライベート）に送信されるトラフィックです。Carbon Black Cloud コンソールで、クラスタから出力グループへの送信トラフィックを確認できます。デフォルトの出力グループは、[パブリック] と [プライベート] です。追加の出力グループを作成できます。出力グループを参照してください。

ネットワーク マップでのクラスタ アクティビティの調査

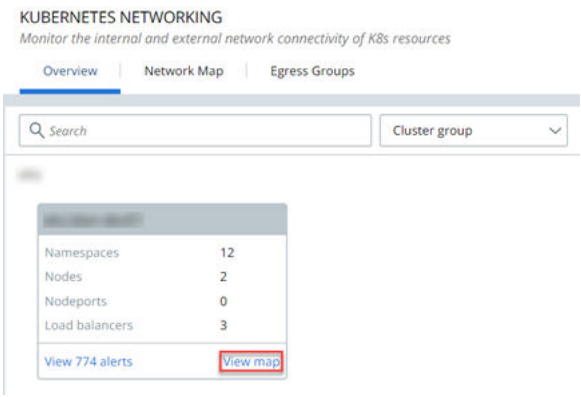
インタラクティブ ネットワーク マップを使用して、Kubernetes クラスタのアクティビティを確認できます。マップのフォーカス（入力方向チャネル、出力グループ、名前空間、またはワークロード）を選択できます。

手順

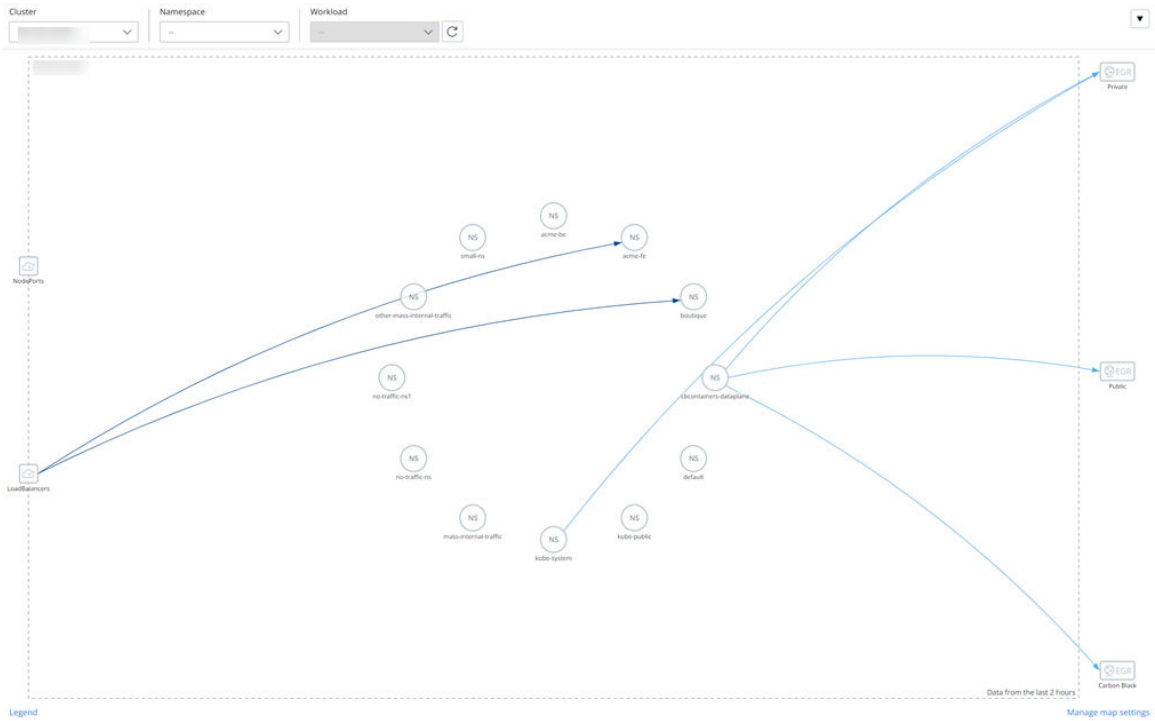
1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [ネットワーク] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [ネットワーク] の順にクリックします。

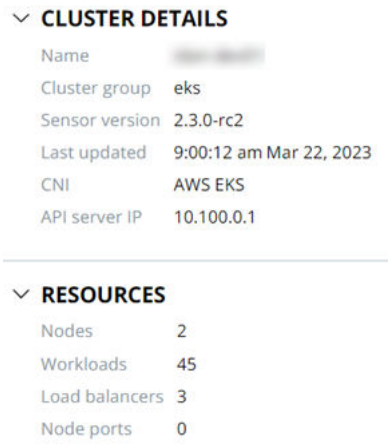
2 [概要] タブで監視するクラスタを選択し、[マップを表示] をクリックします。



- [ネットワーク マップ] タブがアクティブになり、選択したクラスタのデータがロードされます。



- マップの左側には、クラスタで使用可能な入力方向リソース（[NodePort] サービス、[ロード バランサ] サービスなど）が表示されます。特定の入力方向リソースのマップをフィルタリングするには、画面の左側にあるその入力方向リソースのグラフィック要素（例えば、[ロード バランサ]）を選択します。
- マップの右側に出力グループが表示されます。特定の出力グループのマップをフィルタリングするには、そのグループのグラフィック要素（例えば、[パブリック]）を選択します。
- クラスタの詳細、Carbon Black Cloud Kubernetes センサー バージョン、クラスタに割り当てられたリソースを確認するには、マップの右側にあるクラスタの詳細パネルを参照してください。



- マップ内の接続の色は、接続が入力方向、出力方向、名前空間の間、名前空間の内部かを示します。接続をクリックすると、ネットワーク接続の詳細がマップの右側に表示されます。マップの左下にある色の凡例は、各色の接続を定義しています。

3 デフォルトのマップ設定を変更するには、[マップ設定の管理] をクリックし、設定を ON または OFF に切り替えます。

たとえば、リスクにさらされる Kubernetes ネットワークをより効果的に分析するために、暗号化された接続を除外し、暗号化されていない接続のみを監視できます。

- [暗号化された接続を表示] を OFF に切り替えます。
- [暗号化されていない接続を表示] を ON に切り替えます。

ネットワーク マップには、暗号化されていない接続のみが表示されたままになり、調査が容易になります。

ネットワーク マップ上の名前空間データの可視化

Kubernetes インタラクティブ ネットワーク マップには、クラスタ内の名前空間とそのネットワーク接続が表示されます。

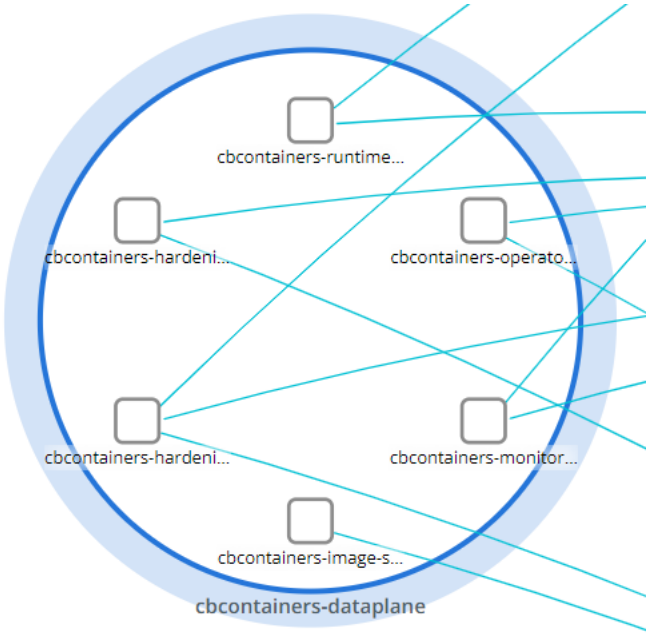
注： システム名前空間はデフォルトで除外されます。マップにシステム名前空間を表示するには、[マップの設定を管理] をクリックし、[システム名前空間を表示] を ON に切り替えます。

システム名前空間:

- kube-system
- kube-public
- cbcontainers-dataplane
- vmware-system
- gatekeeper-system
- tanzu-system
- tanzu-observability-saas

名前空間の詳細を表示するには、マップ内の視覚表示をクリックします。

マップには、選択した名前空間がグラフィカルに表示され、その中で実行されているすべてのワークロードが表示されます。例：

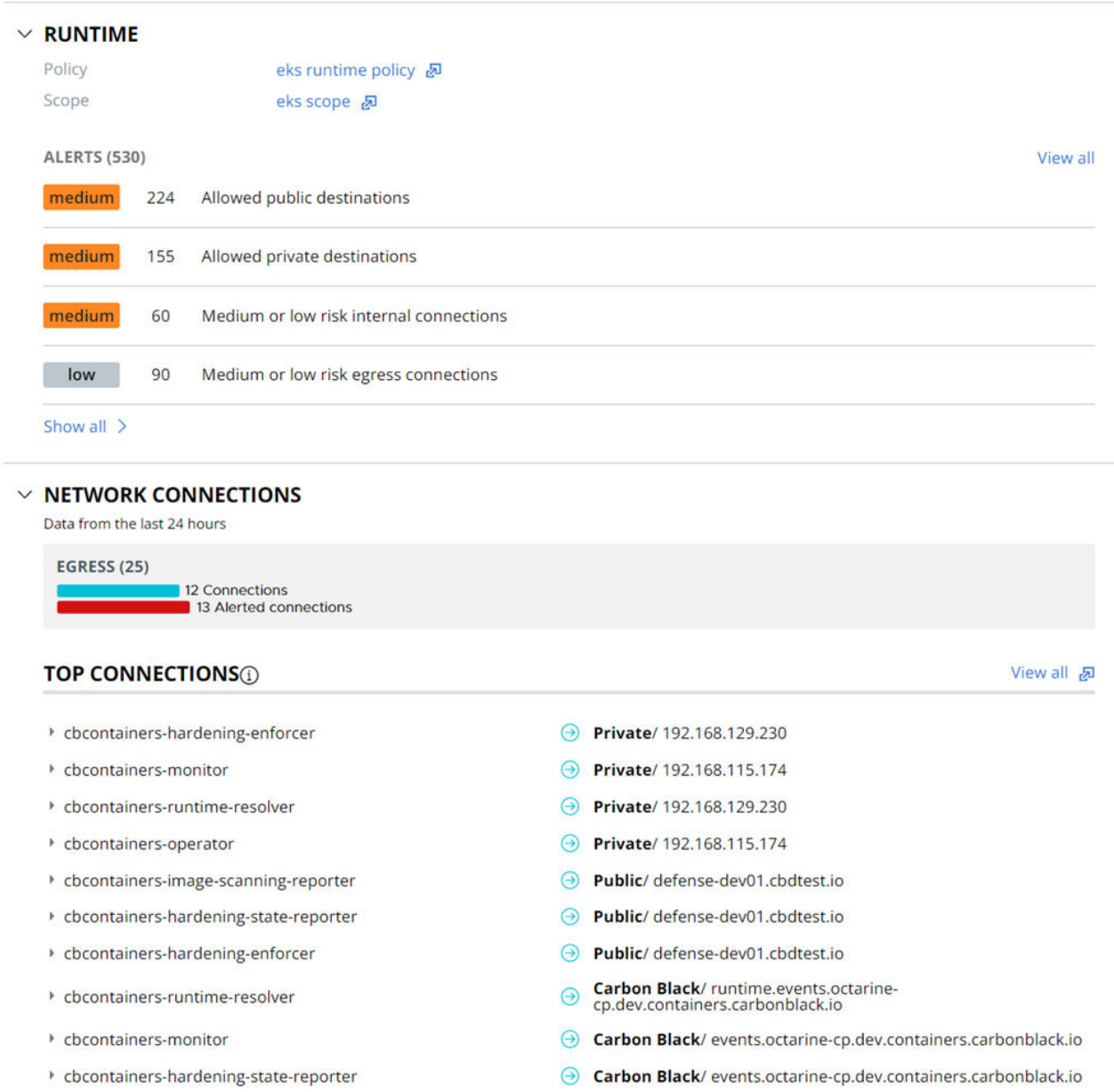


マップ内で以下を実行できます。

- マップの空白の任意の場所をクリックして、クラスタの詳細とリソースを表示します。
- 任意の行をクリックして、アラートが発生したネットワーク接続を表示します。
- ワークロードをクリックして、そのデータを表示します。ネットワーク マップ上のワークロード データの可視化を参照してください。

名前空間の詳細パネル

マップの右側にあるパネルには、その名前空間のすべての出力方向接続および入力方向接続、名前空間を行き来する名前空間トラフィック、名前空間内の内部トラフィックに関する詳細情報が表示されます。



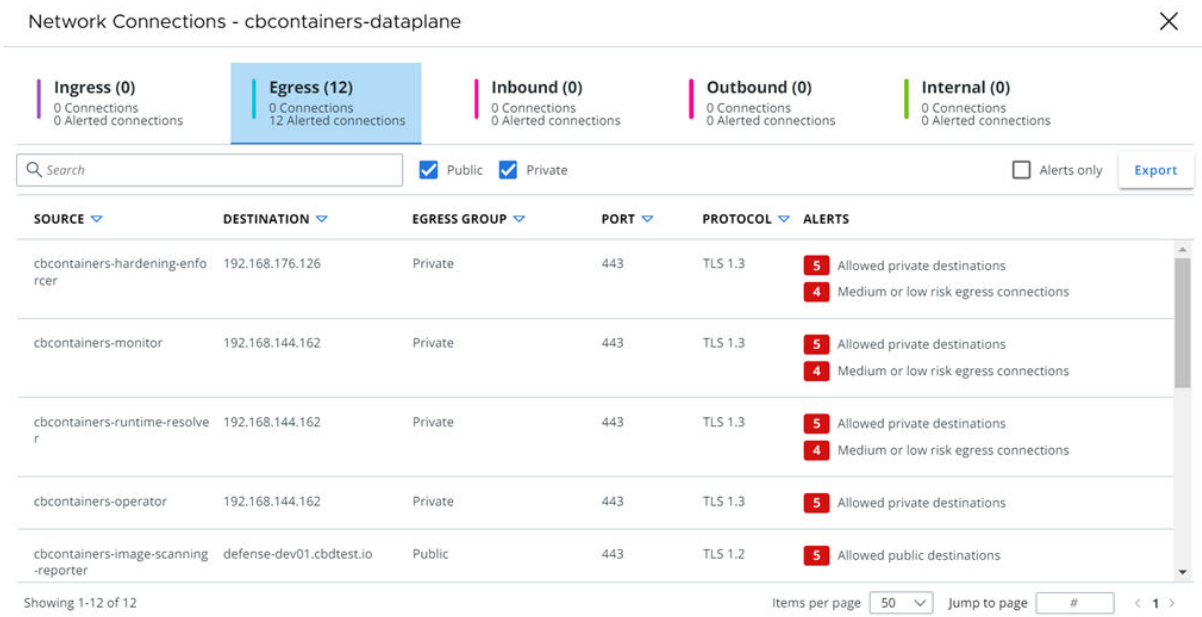
アラートは次の方法で示されます。

- [ランタイム] セクション。
- [ネットワーク接続] セクションの棒グラフ。過去 24 時間のアラート結果が含まれます。
- マップでは、アラートが発生した接続は、その端の感嘆符アイコンで示されます。

このパネルには、次のビューが表示されます。

- 関連付けられたランタイム ポリシーを表示するには、ハイパーリンクされたポリシー名をクリックします。同様に、ハイパーリンクされた範囲名をクリックすると、範囲のサマリの詳細を表示できます。
- パネルの [ランタイム] セクションで [すべて表示] をクリックすると、[アラート] 画面が開き、この名前空間のネットワーク接続アラートが表示されます。

- 追加のネットワーク データを表示するには、パネルの [ネットワーク接続] セクションで [すべて表示] をクリックします。



このパネルでは以下を実行できます。

- 入力方向接続、出力方向接続、インバウンド接続、アウトバウンド接続、および内部ネットワーク接続を表示します。
- 特定のネットワーク接続の検索
- テーブルの結果をフィルタリングします。たとえば、[出力方向] タブでは、[パブリック]、[プライベート] または [アラートのみ] で結果をフィルタリングできます。
- ネットワーク接続データを CSV ファイルにエクスポートします。例えば:


```
{
  "num_found": 12,
  "results": [
    {
      "alerts": [
        {
          "action": "ALERT",
          "rule_id": "ae7b3c4e-4b6b-47fc-847c-8d0c8929c23f",
          "rule_name": "Medium or low risk egress connections",
          "severity": 4
        },
        {
          "action": "ALERT",
          "rule_id": "ec912f66-57c1-466b-b597-1d4a4ce1429c",
          "rule_name": "Allowed private destinations",
          "severity": 5
        }
      ],
      "destination_name": "192.168.176.126",
      "destination_parent_name": "Private",
      "is_private": true,
      "port": 443,
      "protocol": "TLS 1.3",
      "source_name": "cbcontainers-hardening-enforcer",
      "source_parent_name": "cbcontainers-dataplane",
      "type": "EGRESS"
    },
```

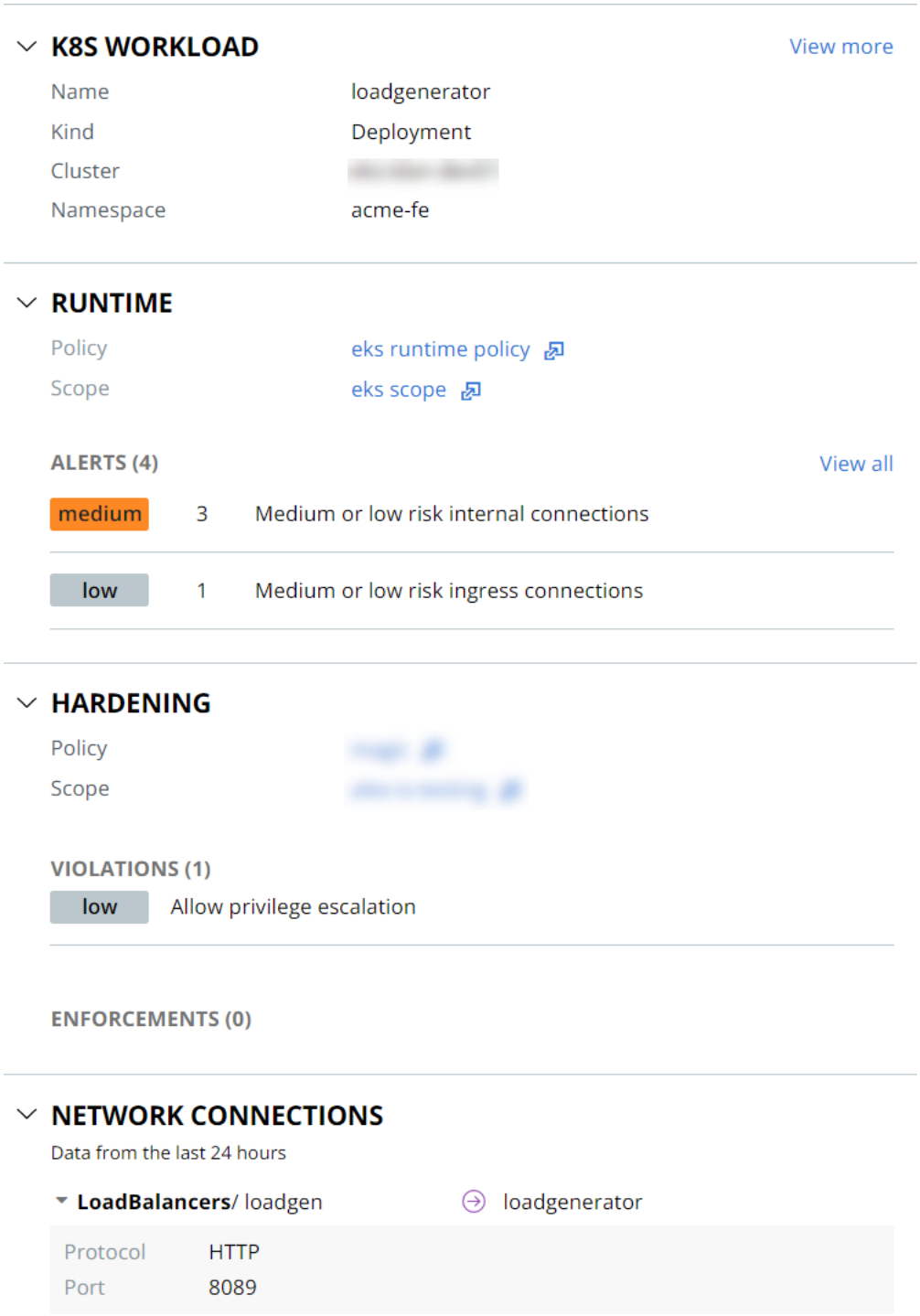

ネットワーク マップ上のワークロード データの可視化

Kubernetes インタラクティブ ネットワーク マップには、クラスタ内のワークロードが表示されます。

ワークロードの詳細情報を表示するには、マップ内のそれぞれのビジュアル要素をクリックします。これは名前空間内のワークロード要素になります。

ヒント: また、マップの上にある [ワークロード] ドロップダウン メニューでワークロードの名前をクリックしてワークロードを選択することもできます。

マップには、指定されたワークロードのみが表示されます。マップの右側のパネルには、ワークロード データのサマリが表示されます。



このパネルには、次のビューが表示されます。

- このワークロードのすべてのデータを表示するには、ネットワーク マップを終了し、[ワークロードの詳細] の横にある [詳細表示] をクリックして特定のワークロードのサマリ画面に移動します。
- パネルの [ランタイム] セクションで [すべて表示] をクリックすると、[アラート] 画面が開き、このワークロードのアラートが表示されます。
- [セキュリティ強化] で、ハイパーリンクされたポリシー名をクリックして、関連付けられたランタイム ポリシーのサマリを表示します。同様に、ハイパーリンクされた範囲名をクリックすると、範囲のサマリの詳細を表示できます。

コンテナのセキュリティ問題の調査と修正

6

コンテナ イメージと脆弱性の確認中に、検出されたコンテナ セキュリティの問題を修正できます。このセクションでは、セキュリティの問題を特定して修正するために実行できる手順について説明します。

次のトピックを参照してください。

- Kubernetes イベントの確認 (セキュリティ強化)
- [調査] 画面でのコンテナ イベントの調査
- [プロセス分析] 画面でのコンテナ イベントの調査
- Kubernetes アラートのトリアージ
- 使用可能な修正とパッチの特定

Kubernetes イベントの確認 (セキュリティ強化)

Kubernetes イベントは、リソースがポリシーに違反するたびに報告されます。ポリシーまたはルールでグループ化し、範囲、クラスタ、およびその他の基準でフィルタリングできます。

次のようにして違反を減らすことができます。

- 環境内の問題を解決する
- 選択したルールの例外を作成する
- 必要に応じてポリシー ルールを変更する

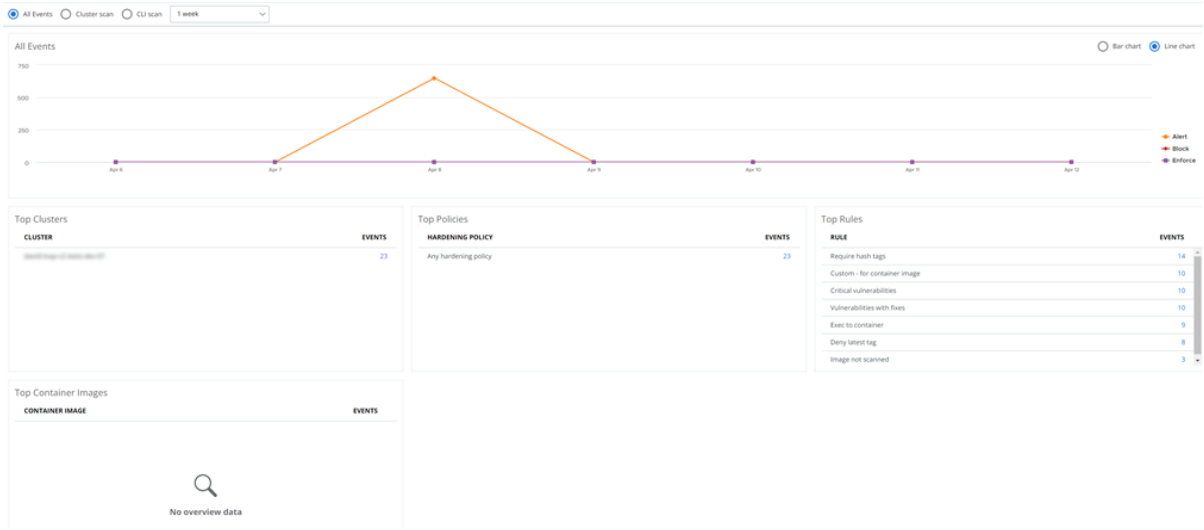
Kubernetes イベントの確認 - 概要

Kubernetes イベントの概要については、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[セキュリティ強化] - [K8s イベント] の順にクリックします。

2 [概要] タブをクリックします。



[概要] タブで、表示するデータとそのデータの表示方法を選択できます。次のオプションを表示します。

- すべてのイベント、クラスタ スキャン イベント、または CLI スキャン イベント
- 1 週間、2 週間、または 1 か月以内に発生したイベント
- 横棒グラフまたは折れ線グラフのイベント データ

イベントの詳細は、[イベント] タブで表示できます (Kubernetes イベントの確認 - 詳細を参照)。詳細情報を取得するイベントを指定するには、次の手順を実行します。

- スキャンされたクラスタのイベントを表示するには、[上位クラスタ] 表で、[イベント] 列の番号をクリックします。[イベント] タブが開き、そのクラスタのイベントが表示されます。
- ポリシーに関連付けられているイベントを表示するには、[上位ポリシー] 表の [イベント] 列の番号をクリックします。[イベント] タブが開き、そのポリシーのイベントが表示されます。
- ポリシー ルールに関連付けられているイベントを表示するには、[上位ルール] 表で、[イベント] 列の番号をクリックします。例：

[イベント] タブが開き、そのルールが表示されます。

- コンテナ イメージに関連付けられているイベントを表示するには、[上位コンテナ イメージ] 表で、[イベント] 列の番号をクリックします。[イベント] タブが開き、そのコンテナ イメージのイベントが表示されます。

Kubernetes イベントの確認 - 詳細

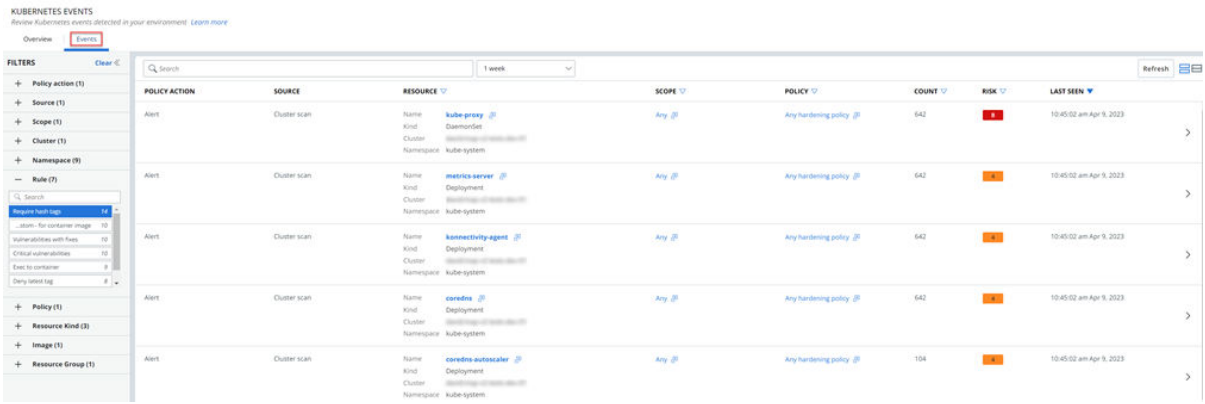
Kubernetes イベントの詳細を表示するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[セキュリティ強化] - [K8s イベント] の順にクリックします。

2 [イベント] タブをクリックします。

この画面には、確認して実行できる Kubernetes イベントのリストが表示されます。



複数の方法でルールのリストを絞り込むことができます。

- 特定の側面（ポリシー ルールやコンテナ イメージなど）にルールをフォーカスします。「Kubernetes イベントの確認 - 概要」を参照してください。
- [検索] バーを使用してイベントを検索します。
- 左側のパネルでフィルタを使用します。複数のファセットを同時にフィルタリングできます。たとえば、ルールとポリシーに一致するイベントのみを含むようにフィルタを設定できます。

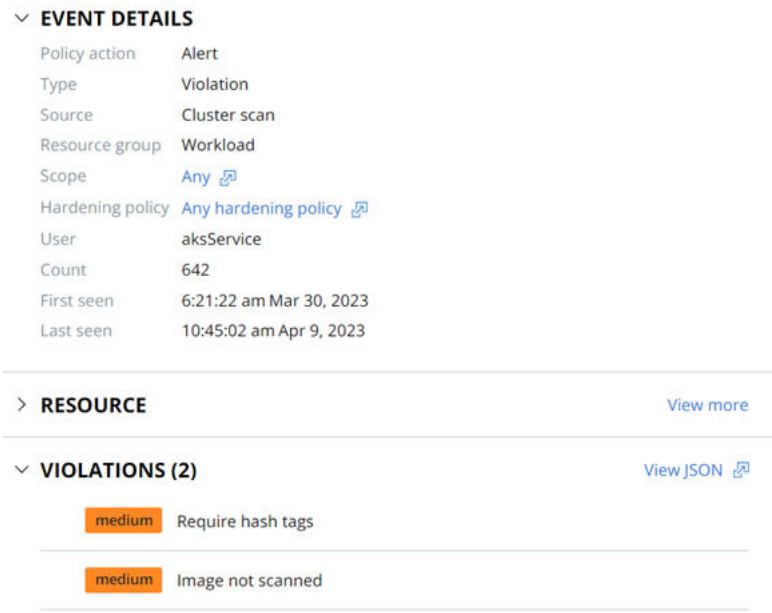
[イベント結果] 表には、デフォルトで次の列が含まれています。

列	説明
ポリシー アクション	イベントを開始したポリシー アクション。これは、アラート、ブロック、または適用です。
ソース	このイベントの検出方法。これは、クラスタ スキャンまたは CLI スキャンのいずれかです。
リソース	Kubernetes リソース タイプ。この列には、このワークロードの名前、種類、クラスタ、名前空間のデータが含まれます。このリソースに関する詳細パネルを開くには、[名前] の横にある アイコンをクリックします。
範囲	このリソースとイベントに関連付けられている範囲。範囲のサマリを表示するには、範囲名の横にある アイコンをクリックします。
ポリシー	このリソースとイベントに関連付けられているポリシー。ポリシーの詳細を表示するには、ポリシー名の横にある アイコンをクリックします。

列	説明
数	ポリシー アクションが原因で発生した同一イベントの数。
リスク	このイベントのリスク重要度。
最後の認識日時	このイベントが最後に検出された時刻。

これらの列をカスタマイズするには、画面の左下にある [表の構成] をクリックします。

イベントの詳細を表示するには、行の右側にある › アイコンをクリックします。



追加画面を開くには、次のリンクを使用できます。

- 範囲のサマリを表示するには、範囲名の横にある アイコンをクリックします。
- ポリシーの詳細を表示するには、ポリシー名の横にある アイコンをクリックします。
- [ワークロード] 画面を開くには、[リソース] セクションで [詳細を表示] をクリックします。
- 違反しているリソースの詳細を JSON 形式で表示するには、[違反] セクションで、 [JSON を表示] の横にある アイコンをクリックします。例：

[調査] 画面でのコンテナ イベントの調査

このセクションでは、Carbon Black Cloud コンソールの [調査] 画面でコンテナ イベントと Kubernetes イベントを調査する方法について説明します。

注： このコンテンツは、コンテナと Kubernetes に固有です。Carbon Black Cloud コンソールの [調査] ページをより詳しく説明した文書は、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの「イベントの調査」「」を参照してください。

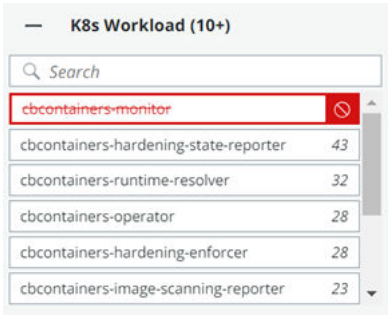
[調査] 画面には、コンテナと Kubernetes のイベントをフィルタリングする 5 つの方法があります。

- ［コンテナ］

- [コンテナ イメージ]
- [Kubernetes クラスタ]
- [Kubernetes 名前空間]
- [Kubernetes ワークロード]

フィルタを組み合わせて特定の結果を得ることができます。

- 縦に並んだ 3 つのドットの [構成] メニューをクリックして、コンソールに表示されるフィルタを構成します。
- フィルタ値の右側にある [除外] アイコンをクリックすると、検索結果を除外できます。例：



注：

- コンテナおよび Kubernetes イベントのリストと検索フィールドについては、次の表を参照してください。
- 使用可能な検索フィールドの完全なリストについては、[調査] ページの右上隅にある製品内『検索ガイド』を開きます。

コンテナ フィールド

表 6-1. アルファベット順のコンテナ フィールド

フィールド名	説明	検索可能かどうか	例
Container Annotations	コンテナ管理者によってコンテナに割り当てられた任意のメタデータのキー値リスト。	いいえ	"com.example.gpu-cores": "2"
Container Engine	コンテナを実行するエンジン（Containerd、Docker、または CRIO）。	いいえ	Docker
Container Engine Version	コンテナ エンジンのバージョン。	いいえ	1
Container ID	コンテナの ID。	はい	f78375b1c487e03c9438c729345e54db9d20cfa2ac1fc3494b6eb60872e74778
Container Image Hash	コンテナ イメージの SHA-256 ハッシュ。	はい	sha256:83d3456789b9a85b98bd162f1ec4d7bc1942f0035caed0f80b3b98a3eab225a7dc

表 6-1. アルファベット順のコンテナ フィールド （続き）

フィールド名	説明	検索可能かどうか	例
Container Image Name	コンテナ イメージの名前。イメージは、コンテナを作成できる実行可能コードを含む静的ファイルです。	はい	docker.io/alpine:latest
Container IP Address	コンテナに割り当てられた IP アドレス。	いいえ	192.168.23.100
Container Name	コンテナの名前。名前は通常、ランタイム エンジンまたはプラットフォームによって生成されます。例：Kubernetes	はい	cbcontainers-node-agent
Container Process PID	オペレーティング システムによって割り当てられるコンテナ プロセス ID。Linux の fork() または exec() プロセス操作の場合は複数値の可能性があります。	はい	2134
Container Root Path	コンテナ イメージのホストのパス。	いいえ	root@someworkloadname-67cf888bcd-gk4jl
Entry Point	コンテナの起動時に実行されるコマンド。	いいえ	/bin/nginx -c /etc/nginx/config.json
Host Name	コンテナのホスト名。	いいえ	
Host Process PID	ホストのプロセス PID。	はい	2345
Mount List	コンテナのマウントされたボリュームのリスト。	いいえ	
Mount Name	コンテナのマウントの名前。	いいえ	mylib
Mount Read/Write	マウントされたファイルまたはディレクトリへのアクセスのタイプ。書き込みアクセスでは、ノード上のファイルを変更できます。	いいえ	RW
Mount Source Path	コンテナのホストにあるデバイス名、ファイル、またはディレクトリ名。	いいえ	/var/lib/somedirectory
Mount Target Path	マウント ポイントの宛先：コンテナ内のパス。	いいえ	/lib/somedirectory
Mount Type	コンテナのマウント タイプ（バインド、ボリューム、tempfs）。	いいえ	tempfs
Privileged Container	実行中のコンテナに対して権限のある機能を有効にするかどうかを定義します。https://github.com/opencontainers/runtime-spec/blob/main/config.md.	いいえ	True
Start Time	コンテナの開始時刻。	いいえ	

Kubernetes フィールド

表 6-2. アルファベット順の Kubernetes フィールド

フィールド名	説明	検索可能かどうか	例
Cluster Name	アラートに関連付けられている Kubernetes クラスタの名前。	はい	ross:aks-test
Namespace	アラートに関連付けられている Kubernetes クラスタ内の名前空間。	はい	Default, kube-system
Replica Name	ワークロード内のポッドの名前	はい	example-workload-1643104800-b2t7f
Workload ID	特定の cluster_name/namespace ペア内のワークロードの ID	はい	example-workload
Workload Kind	ワークロードのタイプ：ポッド、デプロイ、ジョブなど	はい	CronJob,Deployment,DemonSet
Workload Name	特定の cluster_name/namespace ペア内のワークロードの名前	はい	example-workload

Kubernetes ネットワーク セキュリティ フィールド

表 6-3. Kubernetes ネットワーク セキュリティ フィールド (アルファベット順)

フィールド名	説明	検索可能かどうか	例
Connection Type	接続のタイプ：INGRESS、EGRESS、INTERNAL_INBOUND など	はい	EGRESS
Egress Group Name	出力グループの名前	はい	null
IP Reputation	Carbon Black Cloud によって割り当てられたレピュテーション：範囲は 1 ～ 100 (ここで 100 は「信頼できる」です)	はい	74
Port	リスニング ポート：リモートまたはローカル	はい	80
Protocol	プロトコルの名前	はい	HTTP
Remote Domain	リモート ドメインの名前	はい	archive.ubuntu.com
Remote IP	通信のリモート側の IP アドレス	はい	91.189.88.152

調査コンテナ イベント

コンテナに関連付けられているイベントを調査するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[調査] - [プロセス] をクリックします。

2 左側のペインで、 [コンテナ] または [コンテナ イメージ] でフィルタリングします。

3 必要に応じて、[検索] バーで追加のクエリ基準を定義し、**Enter** を押してクエリを実行します。

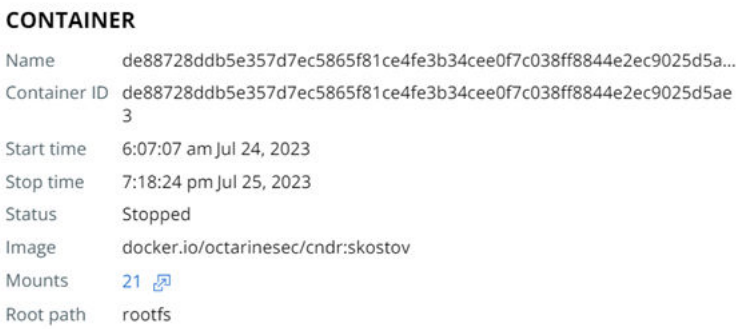
注：

- コンテナおよび Kubernetes イベントのリストと検索フィールドについては、「[調査] 画面でのコンテナ イベントの調査」を参照してください。
- 使用可能なすべての検索フィールドのリストについては、ページの右上隅にある製品内『検索ガイド』を開きます。

4 結果テーブルの特定のイベントの詳細については、アラート行の右側にある矢印

 アイコンをクリックします。

右側のパネルの [コンテナ] セクションには、次の詳細が表示されます。



注： [イベントの詳細] パネルの詳細については、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの 「調査 - プロセス」「」を参照してください。

Kubernetes クラスタの調査

Kubernetes クラスタに関連付けられているイベントを調査するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[調査] - [プロセス] をクリックします。

2 左側のペインで、[K8s クラスタ] でフィルタリングします。

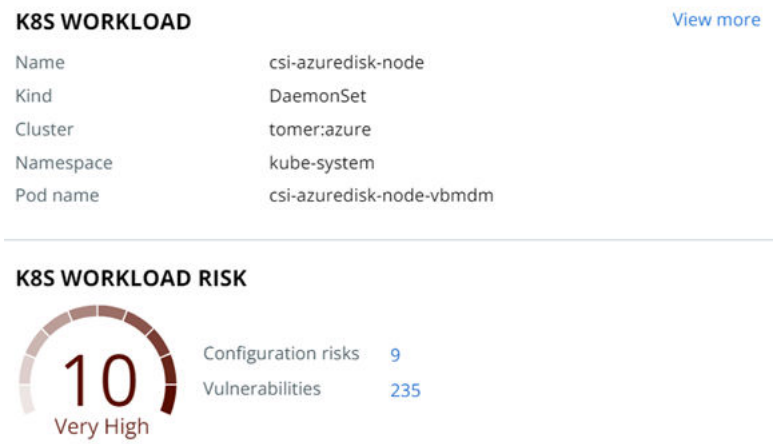
3 必要に応じて、[検索] バーで追加のクエリ基準を定義し、**Enter** を押してクエリを実行します。

注：

- コンテナおよび Kubernetes イベントのリストと検索フィールドについては、「[調査] 画面でのコンテナイベントの調査」を参照してください。
- 使用可能なすべての検索フィールドのリストについては、ページの右上隅にある製品内『検索ガイド』を開きます。

4 結果テーブルの特定のイベントの詳細については、アラート行の右側にある矢印

 アイコンをクリックします。

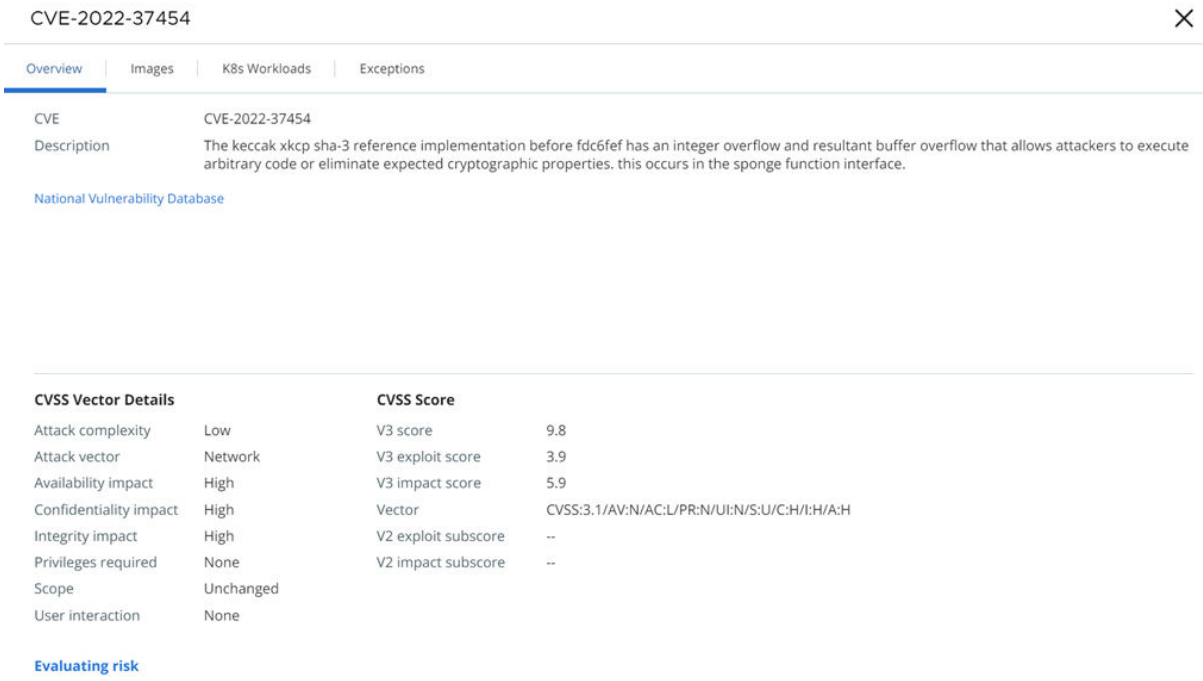


注： [イベントの詳細] パネルの詳細については、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの 「調査 - プロセス」「」を参照してください。

[さらに表示] をクリックして、[Kubernetes ワークロード] 画面を表示します。Kubernetes ワークロードの表示を参照してください。

Kubernetes クラスタ構成の問題を調査するには、[構成のリスク] に関連付けられている番号をクリックします。Kubernetes ワークロードの表示 - リスクを参照してください。

Kubernetes クラスタの脆弱性を調査するには、[脆弱性] に関連付けられている番号をクリックします。この脆弱性の詳細については、「Kubernetes ワークロードの表示 - リスク」を参照し、[脆弱性] 列の任意のリンクをクリックします。例：



Kubernetes 名前空間の調査

Kubernetes 名前空間に関連付けられているイベントを調査するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[調査] - [プロセス] をクリックします。

2 左側のペインで、[K8s 名前空間] でフィルタリングします。

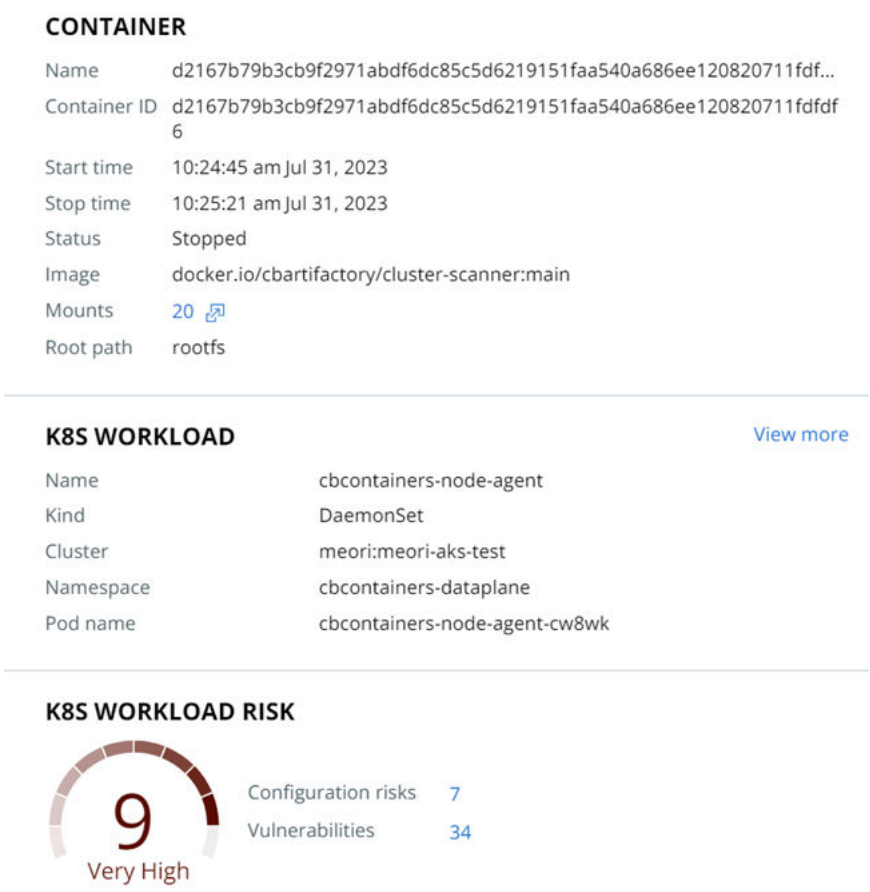
3 必要に応じて、[検索] バーで追加のクエリ基準を定義し、**Enter** を押してクエリを実行します。

注：

- コンテナおよび Kubernetes イベントのリストと検索フィールドについては、「[調査] 画面でのコンテナ イベントの調査」を参照してください。
- 使用可能なすべての検索フィールドのリストについては、ページの右上隅にある製品内『検索ガイド』を開きます。

4 結果テーブルの特定のイベントの詳細については、アラート行の右側にある矢印

アイコンをクリックします。



注： [イベントの詳細] パネルの詳細については、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの 「調査 - プロセス」「」を参照してください。

[さらに表示] をクリックして、[Kubernetes ワークロード] 画面を表示します。Kubernetes ワークロードの表示を参照してください。

Kubernetes クラスタ構成の問題を調査するには、[構成のリスク] に関連付けられている番号をクリックします。Kubernetes ワークロードの表示 - リスクを参照してください。

Kubernetes クラスタの脆弱性を調査するには、[脆弱性] に関連付けられている番号をクリックします。この脆弱性の詳細については、「Kubernetes ワークロードの表示 - リスク」を参照し、[脆弱性] 列の任意のリンクをクリックします。

Kubernetes ワークロードの調査

Kubernetes ワークロードに関連付けられているイベントを調査するには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[調査] - [プロセス] をクリックします。

2 左側のペインで、[K8s ワークロード] でフィルタリングします。

3 必要に応じて、[検索] バーで追加のクエリ基準を定義し、**Enter** を押してクエリを実行します。

注：

- コンテナおよび Kubernetes イベントのリストと検索フィールドについては、「[調査] 画面でのコンテナ イベントの調査」を参照してください。
- 使用可能なすべての検索フィールドのリストについては、ページの右上隅にある製品内『検索ガイド』を開きます。

4 結果テーブルの特定のイベントの詳細については、アラート行の右側にある矢印

アイコンをクリックします。

右側のパネルには、次の情報が表示されます。

注： [イベントの詳細] パネルの詳細については、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの 「調査 - プロセス」「」を参照してください。

[さらに表示] をクリックして、[Kubernetes ワークロード] 画面を表示します。Kubernetes ワークロードの表示を参照してください。

[プロセス分析] 画面でのコンテナ イベントの調査

注： このコンテンツは、コンテナと Kubernetes に固有です。Carbon Black Cloud コンソールの [プロセス分析] ページをより詳しく説明した文書は、VMware Carbon Black Cloud ユーザー ガイドのメイン 調査 セクションの 「プロセス分析」「」を参照してください。

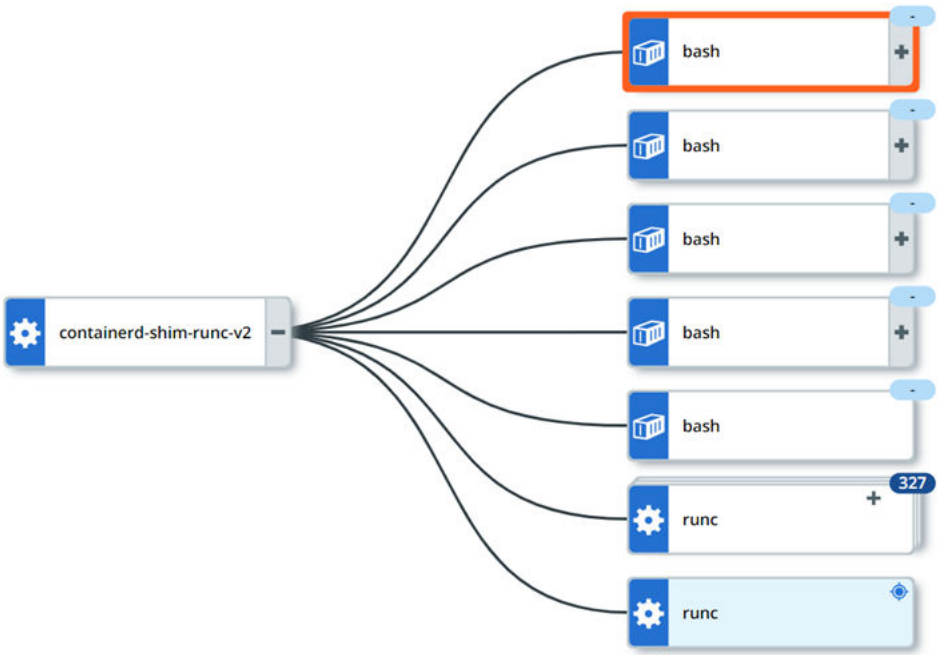
手順

1 左側のナビゲーション ペインで、[調査] - [プロセス] をクリックします。

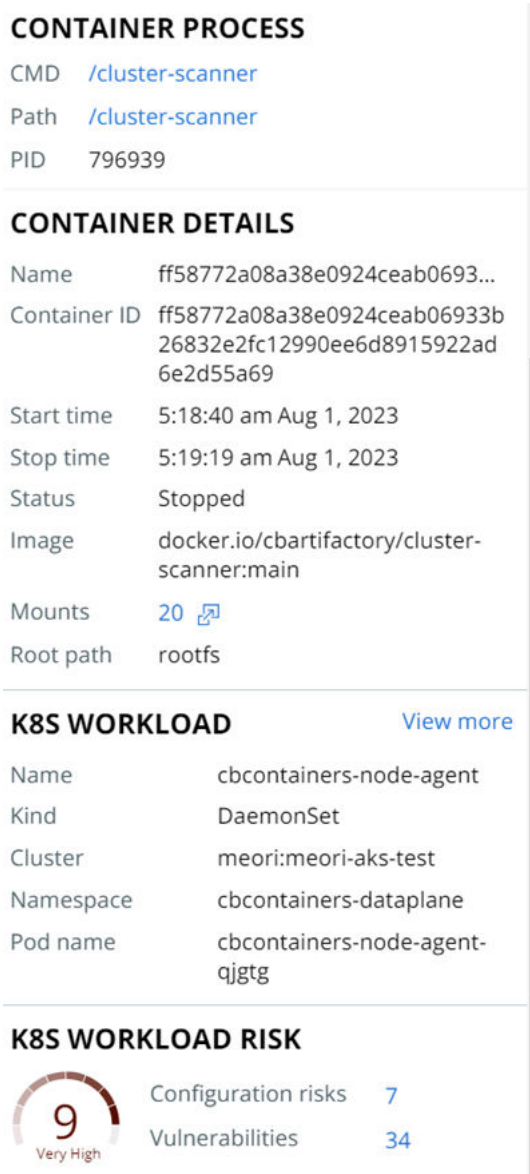
2 コンテナまたは Kubernetes に関連付けられているイベントの検索クエリを実行します。

3 結果テーブルで、行の右側にある [プロセス分析] アイコンをクリックします。

プロセス分析ツリーが表示されます。例：



右側のパネルの情報は、検索して選択したイベントのタイプによって異なります。次のトピックでは、フィルタリングされたイベント タイプ別の選択について説明します。例：



- [さらに表示] をクリックして、[Kubernetes ワークロード] 画面を表示します。Kubernetes ワークロードの表示を参照してください。
- Kubernetes クラスタ構成の問題を調査するには、[構成のリスク] に関連付けられている番号をクリックします。Kubernetes ワークロードの表示 - リスクを参照してください。
- Kubernetes クラスタの脆弱性を調査するには、[脆弱性] に関連付けられている番号をクリックします。この脆弱性の詳細については、「Kubernetes ワークロードの表示 - リスク」を参照し、[脆弱性] 列の任意のリンクをクリックします。

Kubernetes アラートのトリアージ

このセクションでは、Carbon Black Cloud コンソールで Kubernetes アラートをトリアージする方法について説明します。

注： このコンテンツは、Kubernetes アラートに固有のものです。Carbon Black Cloud コンソールでのアラートのトリアージについて詳しく説明しているその他のドキュメントについては、ユーザー ガイドのメイン アラート セクションの「アラート」 「」および「アラートのトリアージ」「」を参照してください。

Kubernetes アラートの検索

Kubernetes ポリシー ルール違反 (アラート) を検索するには、次の手順を実行します。

手順

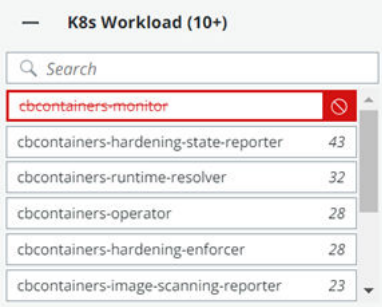
1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 左側のペインのフィルタと [検索] テキスト ボックスを使用して、Kubernetes 違反を検索してフィルタリングします。クエリの構築については、製品内の『検索ガイド』を参照してください。

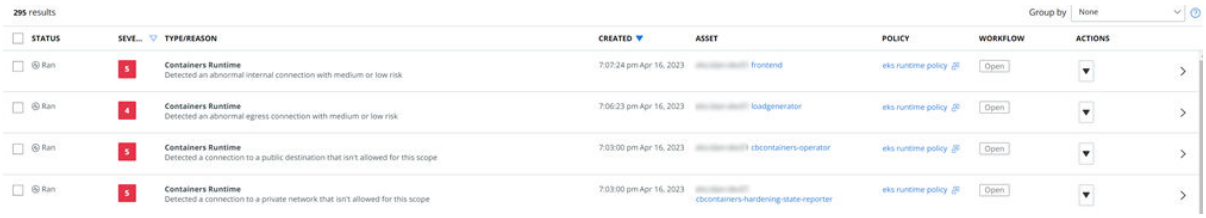
注：

- 時間別に検索結果を定義できます。
- [アラート] 画面には、コンテナと Kubernetes のアラートをフィルタリングする 4 つの方法があります。
  - [K8s クラスタ]
  - [K8s 名前空間]
  - [K8s ワークロード]
  - [K8s ポリシー]

  フィルタを組み合わせて特定の結果を得ることができます。
- 縦に並んだ 3 つのドットの [構成] メニューをクリックして、コンソールに表示されるフィルタを構成します。
- 監視アクション ルールを含むアラートは、デフォルトでは表示されません。これらは、[その他のアクティビティ >観測] フィルタ カテゴリの一部です。
- フィルタ値の右側にある [除外] アイコンをクリックすると、検索結果を除外できます。例：



[検索結果テーブルの例:]



- ワークロードの詳細を表示するには、[アセット] 列でワークロード名をクリックします。Kubernetes ワークロードの表示 - 概要を参照してください。
- ワークロードに割り当てられているポリシーのサマリを表示するには、ポリシー名をクリックします。
- このアラートのプロセス分析ツリーと詳細を表示するには、 プロセス分析 アイコンをクリックします。[プロセス分析] 画面でのコンテナ イベントの調査を参照してください。
- [調査] 画面でアラートを調査するには、調査 アイコンをクリックします。[調査] 画面でのコンテナ イベントの調査を参照してください。
- アラートに対して実行できるアクションの [アクション] ドロップダウン メニューをクリックします。
  - アラートを閉じます。

    重要： アラートを閉じることは、既知の動作を示す特定のワークロードをアラート リストから除外する場合にのみ推奨されます。

  - アラートを進行中としてマークします。
  - アラートに関して送信された通知を表示します。
  - ベースラインにアラートの動作を追加します。ランタイム ポリシーの Kubernetes 範囲ベースラインを参照してください。
- アラートの詳細を表示するには、行の右側にある矢印  アイコンをクリックします。Kubernetes アラートの詳細の表示を参照してください。

Kubernetes アラートの詳細の表示

Carbon Black Cloud コンソールで Kubernetes アラートの詳細を調査するには、次の手順を実行します。

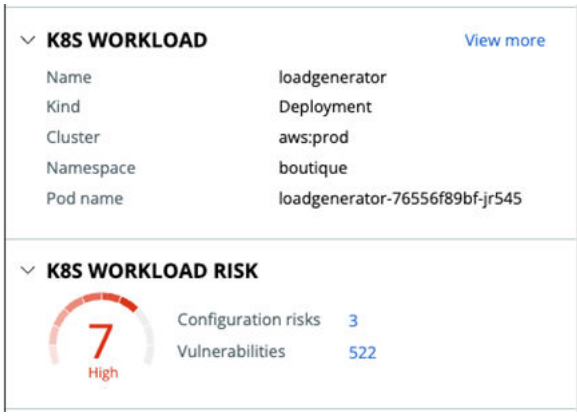
このページでは、Kubernetes アラートの詳細のみを説明します。[アラート] ページの詳細については、VMware Carbon Black Cloud ユーザー ガイドのメイン アラート セクションの 「アラート詳細の表示」「」を参照してください。

前提条件

このトピックでは、Kubernetes アラートを検索し、その検索結果を表示しています。続行する前に、Kubernetes アラートの検索を参照してください。

手順

1 特定のアラートの詳細については、アラート行の右側にある 矢印  アイコンをクリックします。[アラートの詳細] パネルには、次の Kubernetes 情報が含まれています。



2 特定のワークロード画面を開くには、[K8s ワークロード] の横にある [詳細を表示] をクリックします。Kubernetes ワークロードの表示を参照してください。

3 アラートまたはワークロードのあらゆる側面に関する詳細情報にアクセスするには、パネルで関連するハイパーリンクをクリックします。たとえば、[K8s ワークロードのリスク] セクションの [構成リスク] または [脆弱性] の横にある数字をクリックすると、関連するリスクと脆弱性を表示できます。

使用可能な修正とパッチの特定

コンテナ イメージの既知の脆弱性に対して使用可能な修正とパッチを特定できます。

各脆弱性の特徴は次のとおりです。

- CVE コード
- 影響を受けたパッケージまたはライブラリのリスト
- パッケージ バージョン
- 使用可能な修正またはパッチとバージョン

重要： Carbon Black Cloud コンソールで使用可能な修正またはパッチのみを特定できます。適用するには、Kubernetes 環境に進みます。

前提条件

共通脆弱性識別子 (CVE) リスト (外部リンク) について理解します。

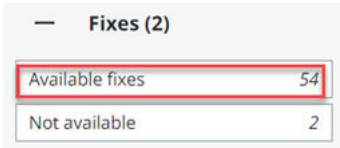
手順

1 左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps または SecOps ロールがあり、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [コンテナ イメージ] の順にクリックします。
- 他のロールがあり、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [コンテナ イメージ] の順にクリックします。

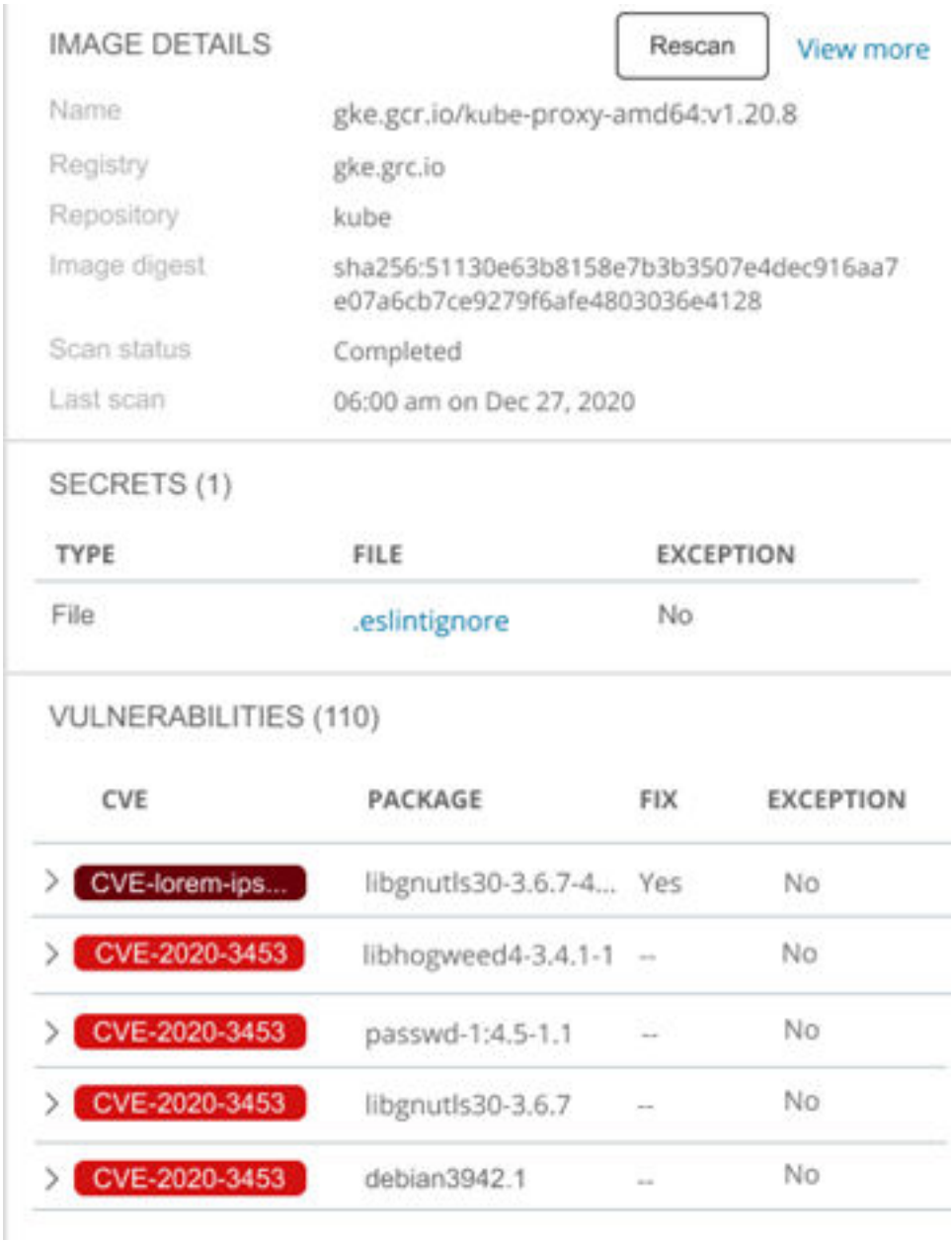
2 [展開されたイメージ] タブを選択します。

3 左側のペインの [修正] フィルタで、[使用可能な修正] を選択します。



この表には、修正があるイメージだけが表示されます。[脆弱性/修正] 列は、関連するカラー バー内の脆弱性の重要度カテゴリ毎の修正数を示します。

4 [イメージの詳細] パネルを展開するには、行の右側にある矢印  アイコンをクリックします。



5 脆弱性が特定された CVE コードとパッケージの簡単な説明を表示するには、[CVE] の左側にある矢印

アイコンをクリックします。

CVE	PACKAGE	FIX	EXCEPTION
CVE-2018-250...	libwebp-dev-0.6....	Yes	Yes
Severity 9.1 Package libwebp-dev-0.6.1-2 Fix 0.6.1-2+deb10u1 Description A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in GetLE16().			
CVE-2018-250...	libwebp6-0.6.1-2	Yes	No
CVE-2018-250...	libwebpdemux2-...	Yes	No
CVE-2018-250...	libwebpmux3-0....	Yes	No
CVE-2018-250...	libwebp-dev-0.6....	Yes	No

次のステップ

それに応じて修正またはパッチを適用します。

クラスタと Kubernetes センサーの管理

7

このセクションでは、セキュリティ環境が起動して実行された後のクラスタと Kubernetes センサーの管理タスクについて説明します。

Carbon Black Cloud で Kubernetes クラスタとセンサーを設定する 手順については、 クラスタの追加と Kubernetes センサーのインストールを参照してください。

次のトピックを参照してください。

- クラスタの表示
- クラスタの編集
- クラスタとそのセンサーの削除
- Kubernetes センサーのアップグレード
- CLI クライアントの削除

クラスタの表示

Carbon Black Cloud コンソールにクラスタを追加したら、クラスタの詳細を表示できます。

前提条件

コンソールにクラスタを追加します。クラスタの追加と Kubernetes センサーのインストールを参照してください。

手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes セキュリティ DevOps ロールが割り当てられており、システムにコンテナ セキュリティ機能のみがある場合、

  [インベントリ] - [クラスタ]を選択します。

- 他のロールが割り当てられており、システムにコンテナ セキュリティとその他の Carbon Black Cloud 機能がある場合、

  [インベントリ] - [Kubernetes] - [クラスタ]を選択します。

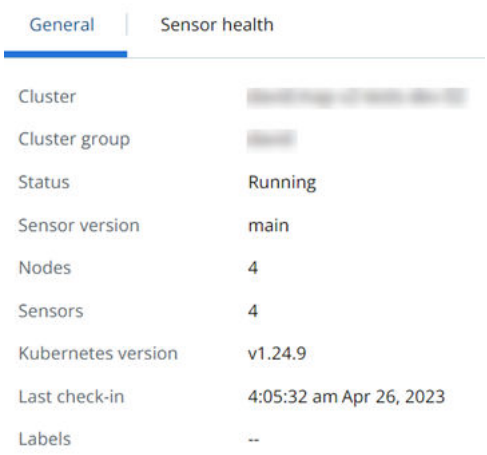
2 [クラスタ] タブをクリックして、[全般] タブをクリックします。

3 左側のペインで、表示されるクラスタのリストを次の方法でフィルタリングできます。

- ステータス
- センサーのバージョン
- オペレータ バージョン
- クラスタ ラベル キー
- クラスタ ラベル値

4 [クラスタ] パネルでは、クラスタを検索できます。また、表示されたクラスタ名を選択して、一般的な情報とセンサーの健全性データの両方を表示できます。センサーの健全性の詳細については、Kubernetes センサーのステータスと健全性の確認 を参照してください。

右側のペインには、次の情報が表示されます。



クラスタの編集

クラスタの設定時に含まれなかった Kubernetes センサーの機能を有効にするには、Carbon Black Cloud コンソールで Kubernetes クラスタを編集します。

前提条件

開始する前に、Carbon Black Cloud コンソールとターミナル ウィンドウの両方を開きます。

手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes セキュリティ DevOps が割り当てられており、システムにコンテナ セキュリティ機能のみがある場合、

  [インベントリ] - [クラスタ]を選択します。

- 他のロールが割り当てられており、システムにコンテナ セキュリティとその他の Carbon Black Cloud 機能がある場合、

  [インベントリ] - [Kubernetes] - [クラスタ]を選択します。

2 編集するクラスタを見つけ、[オプション] ドロップダウン メニューで [編集] をクリックし、[次へ] をクリックします。

3 含める機能を選択します。たとえば、[ランタイム保護]または[クラスタ イメージのスキャン]などです。[次へ] をクリックします。

4 更新を実行するには、[設定の完了] 画面からコマンドをコピーし、ターミナル ウィンドウで実行します。

クラスタとそのセンサーの削除

クラスタから Kubernetes センサーを削除するには、Carbon Black Cloud コンソールからクラスタを削除する必要があります。

前提条件

開始する前に、Carbon Black Cloud コンソールとターミナル ウィンドウの両方を開きます。

手順

1 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes セキュリティ DevOps が割り当てられており、システムにコンテナ セキュリティ機能のみがある場合、

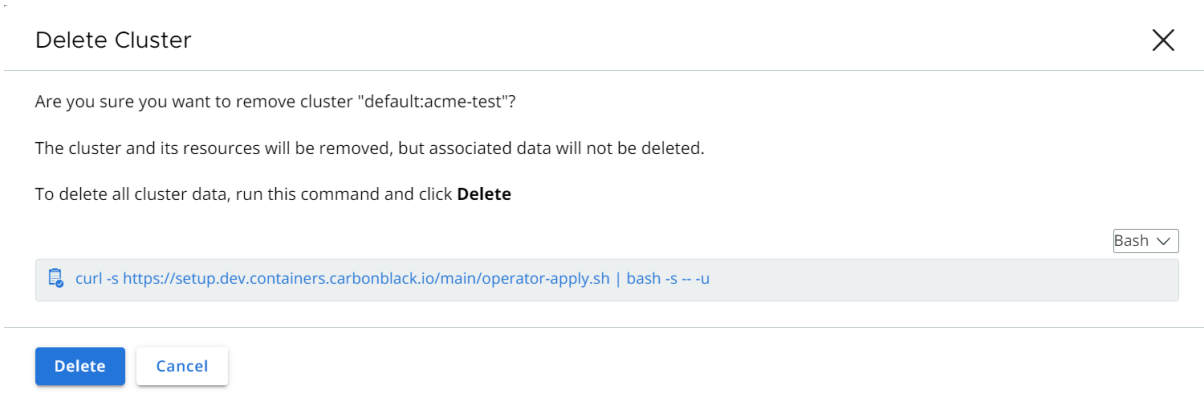
  [インベントリ] - [クラスタ]の順にクリックします。

- 他のロールが割り当てられており、システムにコンテナ セキュリティとその他の Carbon Black Cloud 機能がある場合、

  [インベントリ] - [Kubernetes] - [クラスタ]の順にクリックします。

2 コンソールから削除するクラスタを見つけます。

3 [オプション] ドロップダウン メニューで、[削除] をクリックします。



4 ドロップダウン メニューから [Bash] または [PowerShell] を選択します。

5 コマンドをターミナル ウィンドウにコピーして実行します。

この手順により、Kubernetes センサーと Carbon Black Cloud オペレータがクラスタから削除されます。

重要： 次の手順でコンソールからクラスタを削除せずにコマンドを実行する場合、一定の時間が経過するとクラスタのステータスが [クリティカル] になります。この場合、クラスタを再追加または削除できます。

6 [削除] をクリックします。

重要： 前の手順のコマンドを実行せずに [削除] をクリックすると、Kubernetes センサーと Carbon Black Cloud オペレータはアクティビティなしでクラスタ上に残ります。

Kubernetes センサーのアップグレード

Carbon Black では、最新の Kubernetes センサー バージョンを使用することをお勧めします。

Kubernetes センサーをアップグレードするには、Carbon Black Cloud コンソールか、コマンドライン インターフェイスを使用します。このセクションでは、両方の方法について説明します。

コマンド ラインを使用した Kubernetes センサーのアップグレード

コマンド ラインを使用して Kubernetes センサーをアップグレードできます。

手順

1 ターミナル ウィンドウを開きます。

2 次のコマンドを実行します。ここで、`value` はセンサーの最新バージョンです。

```
kubectl patch cbcontainersagent.operator.containers.carbonblack.io/cbcontainers-agent --
type='json' -p='[{"op": "replace", "path": "/spec/version", "value":"2.2.1”}]
```

注： `cbcontainers-agent` はセンサーを指します。前回のコード ブロックでは、 `2.2.1` は最新のセンサー バージョンです。この値を最新バージョンに置き換えます。

次のステップ

Kubernetes センサーのステータスと健全性の確認

コンソールを使用した Kubernetes センサーのアップグレード

コンソールを使用して Kubernetes センサーをアップグレードできます。

手順

1 ターミナル ウィンドウを開きます。

2 コンソールの左側のナビゲーション ペインで、システム構成とロールに応じて次のいずれかを実行します。

- Kubernetes Security DevOps ロールが割り当てられ、システムにコンテナ セキュリティ機能しかない場合は、[インベントリ] - [クラスタ] の順にクリックします。

- 他のロールが割り当てられ、システムにコンテナ セキュリティ機能とその他の Carbon Black Cloud 機能がある場合は、[インベントリ] - [Kubernetes] - [クラスタ] の順にクリックします。

3 更新するクラスタを見つけます。

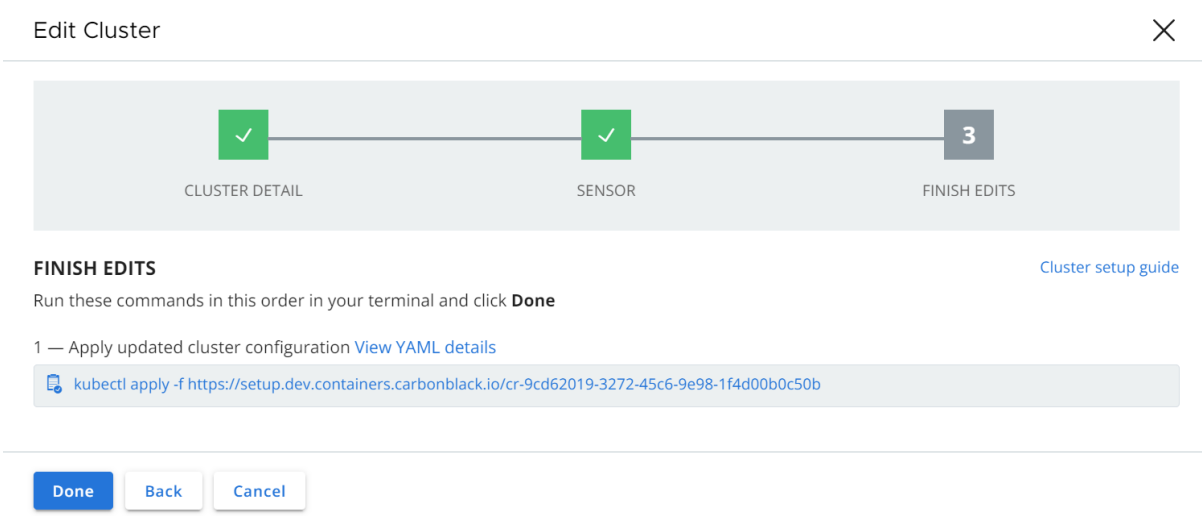
4 [オプション] ドロップダウン メニューで、[編集] をクリックします。

5 必要に応じて、クラスタの新しいラベルを追加します。[次へ] をクリックします。

6 リストから [センサー バージョン] を選択します。これは通常、[バージョン メイン (最新)]である必要があります。

7 以前のセンサー バージョンに含まれていない機能がある場合は、含める機能を選択します。たとえば、[クラスタ イメージのスキャン] などです。[次へ] をクリックします。

8 更新を実行するには、[設定の完了] 画面からコマンドをコピーし、ターミナル ウィンドウで実行します。



9 [完了] をクリックします。

次のステップ

Kubernetes センサーのステータスと健全性の確認

CLI クライアントの削除

使用しなくなった CLI インスタンスを削除できます。

手順

1 左側のナビゲーション ペインで、[インベントリ] > [Kubernetes] > [クラスタ] の順にクリックします。

2 [CLI の構成] タブをクリックします。

3 [アクション] で、削除する CLI クライアントの横にある削除アイコンをクリックします。

結果

CLI クライアントを削除すると、インスタンスと生成された API キーが Carbon Black Cloud から削除されます。環境からインスタンスは削除されません。