コンテナ環境における NIST SP 800-190 コンプライアンスガイド

コンテナの使用における脅威の状況を理解する

組織はコンテナ、Kubernetes、マイクロサービスの導入に熱心に取り組んでいますが、最新の Kubernetes セキュリティレポート[1]によって明らかになったように、セキュリティ上の懸念がその阻害要因となる可能性があります。多くの組織がコンテナを採用していますが、コンテナと Kubernetes 自体についてまだ学習中の組織もあり、このインフラストラクチャがセキュリティに与える影響により、習熟に必要な時間や労力がさらに増加することを理解しています。重要なのは、それらの環境における脅威の状況を理解し、コンテナ使用時のリスクポスチャを評価して、コンテナ導入に伴うセキュリティリスクを軽減することです。

コンテナを保護する方法への理解を深めるためのツールの 1 つが、国立標準技術研究所 (NIST) から提供されている、NIST Special Publication (SP) 800-190[2] です。このツールでは、コンテナ・テクノロジーに関連するセキュリティ上の懸念事項のいくつかを説明し、コンテナ化されたアプリケーションと、関連するインフラストラクチャ・コンポーネントを保護するための実践的な推奨事項を提供しています。

本ガイドを読むことで、NIST SP 800-190 の主要な推奨事項を理解し、当社のお客様が NIST SP 800-190 に準拠するために使用しているソリューションの詳細な説明を確認することができます。

Red Hat OpenShift Platform Plus

Red Hat® OpenShift® Platform Plus は、アプリケーションを大規模にビルド、モダナイズ、デプロイするための統合プラットフォームです。マルチクラスタのセキュリティ、コンプライアンス、アプリケーション、およびデータ管理が複数のインフラストラクチャにわたって機能し、ソフトウェア・サプライチェーン全体で一貫性を提供します。OpenShift Platform Plus は、ハイブリッドクラウド環境でのアプリケーションの市場投入に必要なサービス一式を備えており、作業の最適化と迅速化に役立ちます。

- OpenShift Platform Plus には以下が含まれます。
- Red Hat OpenShift Container Platform
- Red Hat Advanced Cluster Security for Kubernetes
- Red Hat Advanced Cluster Management for Kubernetes
- Red Hat OpenShift Data Foundation
- Red Hat Quay

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

1 Red Hat レポート。「Kubernetes adoption, security, and market trends report 2023」、2023 年 4 月 17 日。
2 NIST。「National Institute of Standards and Technology Special Publication 800-190」。2024 年 5 月 8 日にアクセス。

Kubernetes のセキュリティの概要

Kubernetes 環境でコンテナ化されたアプリケーションを最も効果的に保護する方法は、コンテナのライフサイクルの各フェーズ (ビルド、デプロイ、ランタイム) にセキュリティ制御を組み込むことです。

ビルド

このフェーズで重点が置かれるのは、開発者が作成するコンテナイメージ内に何を含めるかということです。ビルドフェーズでのセキュリティへの取り組みは通常、ベストプラクティスを適用し、既知の脆弱性を早期に特定して排除することで、コンテナのライフサイクル後半のビジネスリスクを軽減することに重点が置かれます。

デプロイ

デプロイフェーズでは、開発者は実稼働環境にデプロイするために、コンテナ化されたアプリケーションを構成します。コンテキストには、イメージに関する情報だけでなく、サービスで使用できる Kubernetes 構成オプションの詳細も含まれます。このフェーズでのセキュリティへの取り組みは、多くの場合、運用上のベストプラクティスの遵守、最小権限の原則の適用、構成ミスの特定が中心となり、これらによって潜在的な侵害の可能性と影響を軽減します。

ランタイム

コンテナは、ライブデータを扱い、ライブユーザーに使用される状態で、社内インターネットや公共インターネットなどのネットワークに公開され、運用が開始されます。ランタイムフェーズにおけるセキュリティの主な目的は、悪意のある攻撃者をリアルタイムで検出して阻止することにより、実行中のアプリケーションと Kubernetes インフラストラクチャの両方を保護することです。

ライフサイクル全体にわたってコンテナを保護するとともに、基盤となるインフラストラクチャも保護し、適切に構成されていることを確認する必要があります。組織にとって、コンテナはワークロードレベルできめ細かいセキュリティを実装するのに役立ちます。しかし同時に、コンテナによって新しいインフラストラクチャ・コンポーネントや未知の攻撃対象領域も導入されます。そのため、クラスタ・インフラストラクチャ、Kubernetes オーケストレーター、およびそれらが実行するコンテナ化されたアプリケーションをセキュリティで保護する必要があります。

OpenShift Platform Plus が NIST SP 800-190 をサポートする仕組み

OpenShift Platform Plus は、アプリケーションを大規模にビルド、モダナイズ、デプロイするための統合プラットフォームです。以下に示す詳細は、OpenShift Platform Plus の機能を、NIST SP 800-190 で提供されるガイダンスにマッピングしたものです。

NIST Standard 4.1.1 - イメージの脆弱性

組織は、コンテナ向けに設計されたイメージ脆弱性ツールを使用する必要があります。効果的なツールとプロセスの主な特徴は次のとおりです。

1. イメージのライフサイクル全体との統合。
2. 組織全体のイメージの全レイヤーにおける脆弱性の一元的な可視化と、組織のビジネスプロセスに合わせた柔軟なレポートおよびモニタリングビュー。
3. ポリシー要件を満たす特定のイメージの進行だけを許可する、ポリシー駆動型の適用。

ソリューション

Red Hat Quay：

1. Clair により、多数の脆弱性データベースを使用してイメージの脆弱性をスキャンし、イメージ内の既存の脆弱性を見つけることができます。
2. また Clair は、オープンソース脆弱性 (OSV) データベースを通じて、golang、Java、および Ruby エコシステムの脆弱性とセキュリティ情報を報告します。

Red Hat Advanced Cluster Management：

1. 複数のクラスタ全体の構成管理に、拡張可能なポリシーフレームワークを使用します。
2. 配置ルールを使用して、ポリシーを管理対象クラスタにバインドします。
3. Compliance Operator との統合をサポートします。
4. Gatekeeper、Open Policy Agent (OPA)、Kyverno など、複数のポリシーエンジンをサポートします。
5. GitOps デプロイによるポリシーをサポートします。
6. ハードウェアおよびソフトウェアスタック全体に適用されます。
7. セキュリティ、レジリエンシー、およびソフトウェアエンジニアリング制御に関する、すぐに使用できるポリシーを提供します。これらは Compliance Operator からは提供されません。

Red Hat Advanced Cluster Security：

1. 継続的インテグレーション/継続的デリバリー (CI/CD) パイプラインとの統合により、開発サイクルのあらゆる段階でイメージ内の脆弱性をスキャンして検出します。
2. エグゼクティブレベルの概要ビューと詳細レポートにより、ベースレイヤーだけでなくすべてのレイヤーのイメージのイントロスペクションを実行します。
3. ポリシーに準拠する特定のイメージの進行だけを許可する、すぐに使用できるポリシーを備えています。

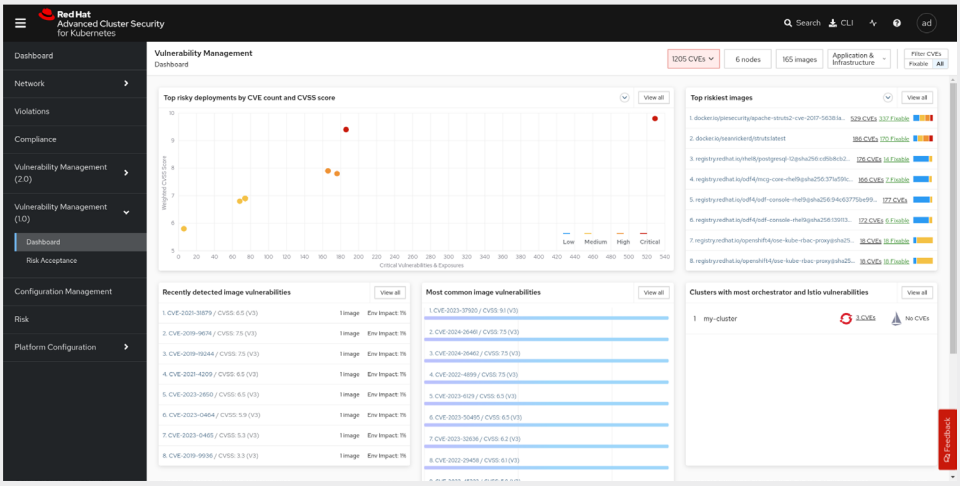

図 1. Red Hat Advanced Cluster Security の脆弱性管理ダッシュボード

4.1.2 - イメージ設定の不具合

組織は、セキュリティを重視した構成のベストプラクティスに確実に準拠するセキュリティ制御とプロセスを実装する必要があります。これには以下が含まれます。

1. イメージ構成設定の監査機能。
2. イメージのコンプライアンス状態に関するリアルタイムおよび継続的なレポートと監視。
3. コンプライアンス違反のイメージの実行を防ぐポリシーの適用。

ソリューション

Red Hat Advanced Cluster Security：

1. 画像スキャンをネイティブにサポートし、既存の画像と統合することもできます。
2. イメージとコンテナの構成を監査し、すぐに使えるポリシーを提供します。このポリシーにより、root ユーザーとしてデプロイされた特権コンテナまたはイメージのインスタンスなどの構成ミスを検出できます。または、組織のニーズに合わせてカスタムポリシーと適用アクションを構成して、イメージがすべてのセキュリティ要件を確実に満たすようにすることもできます。
3. デプロイされたすべてのイメージをリアルタイムかつ継続的に可視化および監視し、ランタイムだけでなくビルドやデプロイの段階でもコンプライアンスを確保します。ポリシーに違反しているイメージまたはコンテナの実行を阻止します。
4. コンテナ内での Secure Shell (SSH) プロトコルの使用を識別する組み込み機能を提供します。これには、ポート 22 の公開や SSH デーモンと思われるプロセスについて警告するポリシーが含まれます。

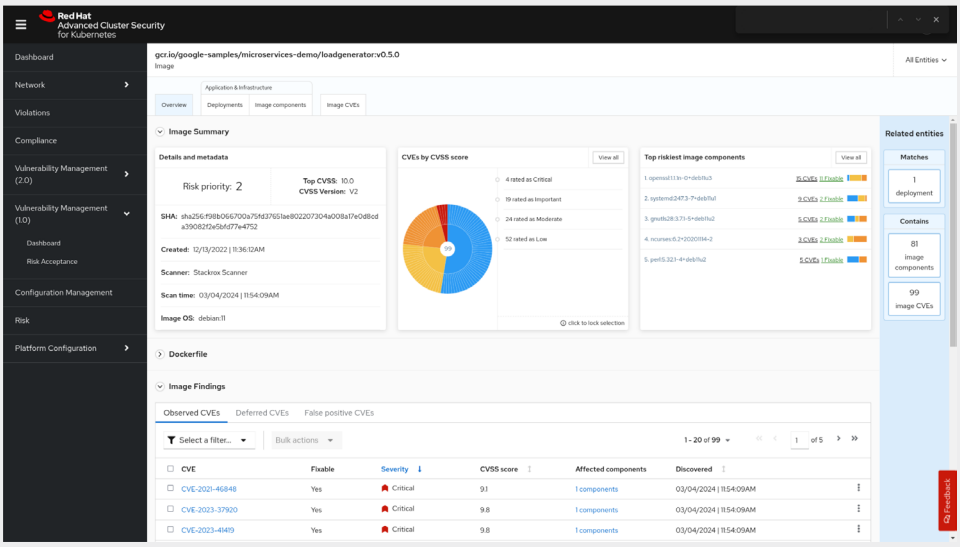

図 2. イメージのサマリー詳細

4.1.3 埋め込まれたマルウェア

組織は、マルウェアが埋め込まれていないかを確認するために、イメージを継続的に監視する必要があります。監視プロセスには、マルウェアのシグネチャセットの使用と、主に実際に「被害が出ている」攻撃に基づいた動作検出ヒューリスティックを含める必要があります。

ソリューション

OpenShift Container Platform：

1. File Integrity Operator により、継続的にクラスタノード上でファイル整合性チェックが実行されます。
2. Advanced Intrusion Detection Environment (AIDE) を使用するデーモンセットをデプロイし、デーモンセットポッドの初回実行中に変更されたファイルのログをステータスオブジェクトに提供します。

Red Hat Advanced Cluster Security：

1. マルウェアが埋め込まれていることによって見られるような、悪意を示す異常なアクティビティを検出します。
2. 安全でないレジストリが使用されないようにするための、すぐに使用できるポリシーを提供します。

4.1.4 - 埋め込まれた平文の秘密情報

組織は、秘密情報をイメージの外部に保存して保護し、ランタイム時にのみ動的にアクセスできるようにする必要があります。組織は秘密情報の管理に Kubernetes を使用して、秘密情報を必要とする特定のコンテナにのみ情報を提供し、保管中および転送中は常に暗号化しておく必要があります。

ソリューション

Red Hat Advanced Cluster Security：

1. 安全でない方法 (環境変数など) で秘密情報を配信しているインスタンスを検出する、すぐに使えるポリシーを提供します。
2. 監視対象のクラスタ内に構成された秘密情報に関するメタデータ (それらの秘密情報を参照するように構成されたデプロイメントを含む) を検査します。
3. Kubernetes 経由で送信された秘密情報に、その情報を使用するよう構成されたコンテナのみがアクセスできるようにします。

4.1.5 - 信頼できないイメージの使用

組織は、信頼できるイメージとレジストリのセットを維持し、このセットのイメージのみが環境内での実行を許可されるようにする必要があります。これにより、信頼できないコンポーネントや悪意のあるコンポーネントがデプロイされるリスクを軽減できます。

ソリューション

OpenShift Container Platform：

1. Red Hat Container Registry 内のイメージのシグネチャを提供します。このシグネチャは、Machine Config Operator (MCO) を使用して OpenShift Container Platform 4 クラスタにプルされるときに自動的に検証できます。
2. 顧客が sigstore を使用して独自のイメージを作成して署名し、OpenShift Container Platform へのデプロイを許可する前にそれらの署名を検証できるようにします。
3. Trusted Artifact Signer は、ソフトウェア開発者と消費者がソフトウェア・アーティファクト (ソースコード、リリースファイル、イメージ、バイナリー、SBOM、プレイブックなど) に安全に署名して検証できるようにし、ソフトウェア・サプライチェーンのセキュリティを強化します。

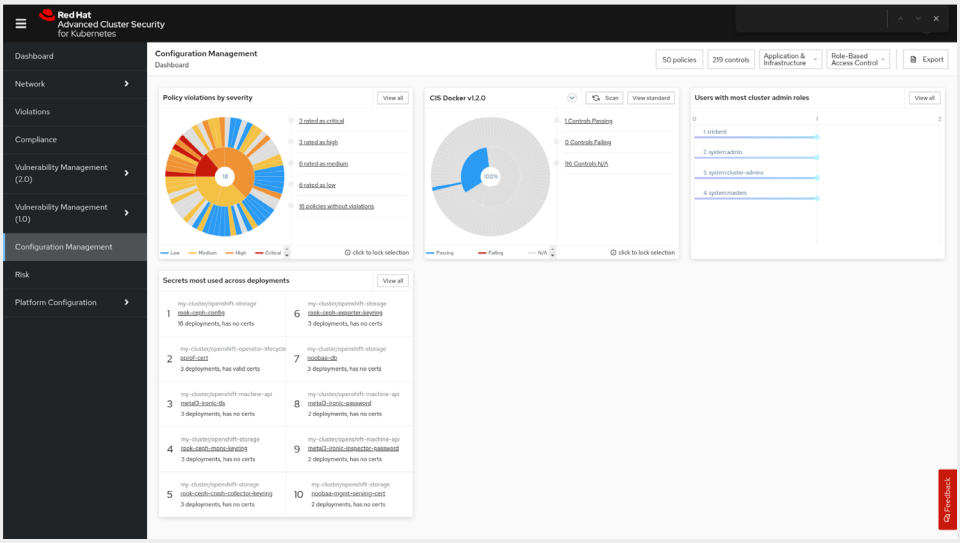

図 3. 構成管理ダッシュボード

4.2.1 - レジストリへのセキュアでない接続

レジストリへのプッシュおよびプルには、安全な接続または暗号化された接続を使用します。

ソリューション

Red Hat Advanced Cluster Security：

1. デフォルトでは、CRI-O エンジンは暗号化されていないレジストリからは取得しません。ただし、安全でない接続が使用されているレジストリをホワイトリストに登録するオプションは用意されています。Red Hat Advanced Cluster Security は、クラスタノード上の CRI-O エンジンの設定を分析し、暗号化されていないレジストリがホワイトリストに登録されている例外を特定します。
2. このソリューションは、イメージのタグまたは参照が http:// で始まる場合にフラグを立てます。

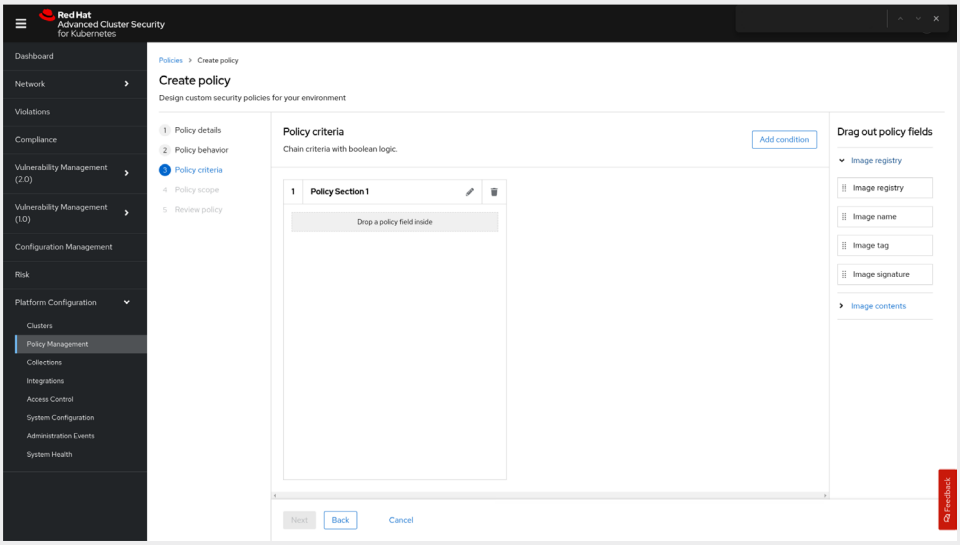

図 4. ポリシーの作成

4.2.2 - レジストリ内の古いイメージ

組織は、最新バージョンのイメージが使用されていることを確認するためのプロセスと制御を実装する必要があります。

ソリューション

Red Hat Advanced Cluster Security：

1. このソリューションには、最新のタグの使用を阻止することを目的とする、事前構築されたポリシーが備えられており、最新のタグの代わりにイメージのバージョンを含む不変の名前を使用してイメージにアクセスすることを推奨します。
2. また、90 日以上前に構築されたイメージの使用にフラグを立てる、すぐに使えるポリシーも用意されています。特定のニーズに合わせて、それよりも短期または長期の時間枠で検出するようにポリシーを構成することもできます。
3. さらに、各デプロイメントのリスクスコアを提供する際には、リスク要因の 1 つとして、イメージが構築されてからの期間が組み込みまれます。

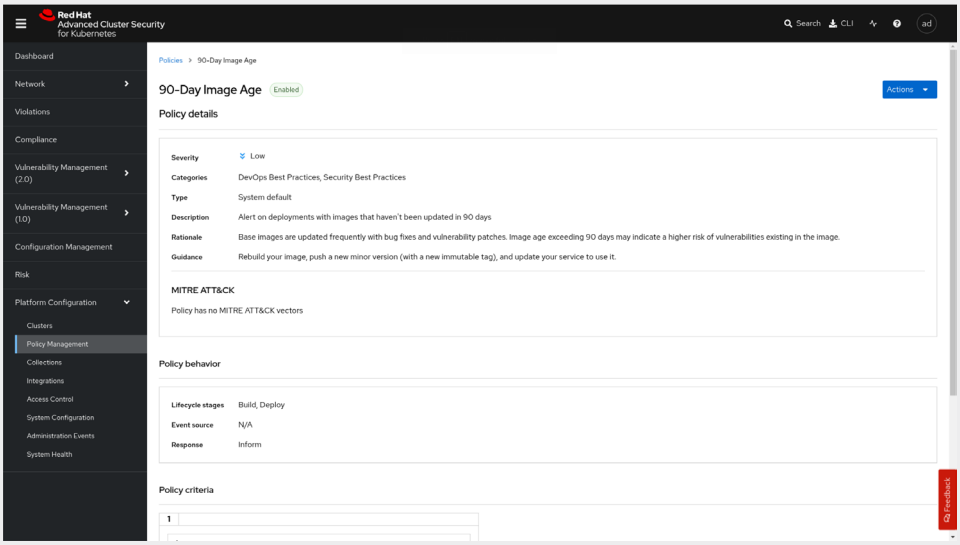

図 5. イメージの 90 日間経過ポリシーの詳細

4.2.3 - 不十分な認証および認可制限

独自のイメージまたは機密イメージを含むレジストリへのすべてのアクセスには認証が必要です。

ソリューション

Red Hat Quay：

1. リポジトリのロールベースのアクセス制御 (RBAC) をサポートし、組織がリポジトリの読み取り、書き込み、管理アクセスを許可および制限できるようにして、独自のイメージや機密イメージを保護します。
2. Red Hat のシングルサインオン・テクノロジー、Google、GitHub、Microsoft などの OpenID Connect プロトコル (OIDC) メソッドの統合をサポートします。

4.3.1 - 無制限の管理アクセス

オーケストレーターは、ジョブロールに必要な特定のホスト、コンテナ、およびイメージ上で特定のアクションを実行する機能のみをユーザーに付与する、最小限のアクセス権限モデルを使用する必要があります。

ソリューション

OpenShift Container Platform：

1. クラスタ管理者は、より多くの特権ロールをユーザーに付与する必要があります。
2. プロジェクトごとにチームを分割できます。
3. 個々の名前空間とプロジェクトに対する RBAC が可能になります。

4.3.2 - 許可されていないアクセス

クラスタ全体の管理アカウントは環境内のすべてのリソースに影響を与える機能を提供するため、これらのアカウントへのアクセスは厳密に制御する必要があります。組織は、パスワードだけでなく多要素認証を要求するなど、強力な認証方法を使用する必要があります。

ソリューション

OpenShift Platform Plus：

- 幅広いプラットフォームにわたり、Red Hat のシングルサインオン・テクノロジーなど、OIDC プロバイダーをサポートします。

4.3.3 - コンテナ間ネットワークトラフィックの不十分な分離

ネットワークトラフィックをセグメント化してリスクを軽減するように Kubernetes を構成します。最初のステップとして、機密レベルごとにネットワークを定義し、機密ネットワークと非機密ネットワークを確実に分離する必要があります。

たとえば、インターネットに広く公開されたアプリケーションは仮想ネットワークを共有し、内部向けのアプリケーションは別のネットワークを使用し、この 2 つの間の通信は少数の明確に定義されたインターフェイスを通じて行われるようにする必要があります。

ソリューション

Red Hat Advanced Cluster Security：

1. Kubernetes ネットワーク・セグメンテーションルールがすべてのデプロイメントに適用されているかどうかのチェックを実行します。
2. ネットワークトポロジを理解できるように、既存のネットワーク接続の視覚的なシミュレーションを提供します。ネットワークグラフは、許可されたアクティブな接続を識別し、アプリケーション間のセグメンテーション・ポリシーのギャップを特定するのに役立ちます。
3. オンデマンドのネットワークポリシー (YAML ファイル) を生成し、それを Kubernetes デプロイメントにプッシュして、ネットワーク・セキュリティポスチャを強化します。

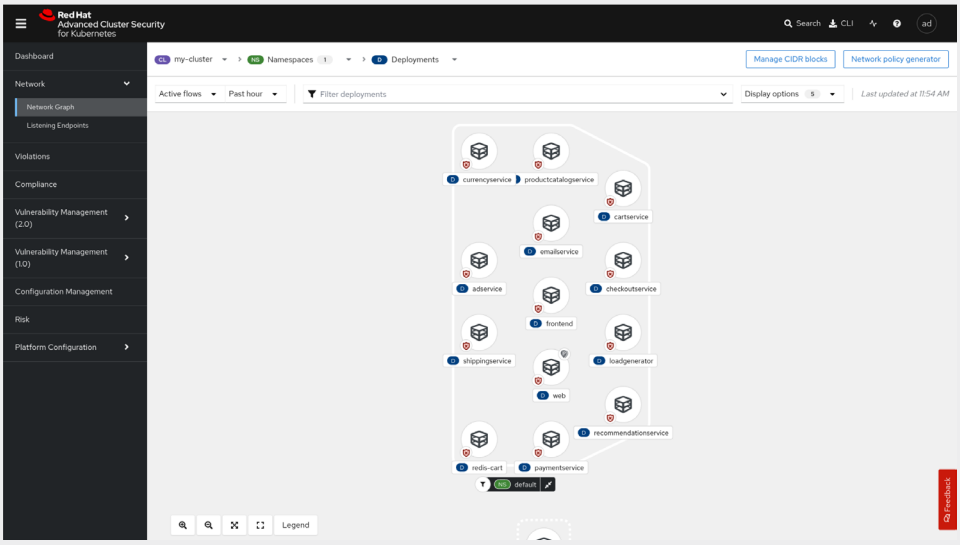

図 6. ネットワークグラフ

4.3.4 - ワークロードの機微性レベルの混合

オーケストレーターは、機密レベルによって特定のホストセットへのデプロイメントを分離するように構成する必要があります。

ソリューション

OpenShift Container Platform：

- OpenShift Container Platform 内でテイントを使用します。

Red Hat Advanced Cluster Security：

- セキュリティポリシーをホストが適用できるようにします。

Red Hat Advanced Cluster Management：

1. セキュリティ、レジリエンシー、およびソフトウェアエンジニアリング制御に関する、すぐに使用できるポリシーを提供します。これらは Compliance Operator からは提供されません。
2. ポリシーの共同開発のための、アクティブなアップストリーム・コミュニティをサポートします。

4.3.5 - オーケストレーターのノードの信頼

Kubernetes デプロイメントでは、ノードをクラスタに安全に導入し、ノードに対してライフサイクルを通じて永続的な ID を付与し、ノードとその接続状態の正確なインベントリを表示する必要があります。クラスタ全体のセキュリティを損なうことなく、個々のノードの侵害に対するレジリエンスを備えた Kubernetes を構成します。運用全体に悪影響を与えることなく、侵害されたノードを隔離して削除します。

ソリューション

Red Hat Advanced Cluster Security：

1. 上記のポリシーに対してデプロイメントのスキャンを実施したかどうかを確認します。
2. スキャンされていないデプロイメントにフラグを立てます。
3. ポリシー違反を特定します。
4. Kubernetes 環境を強化する追加の機会を提供します。

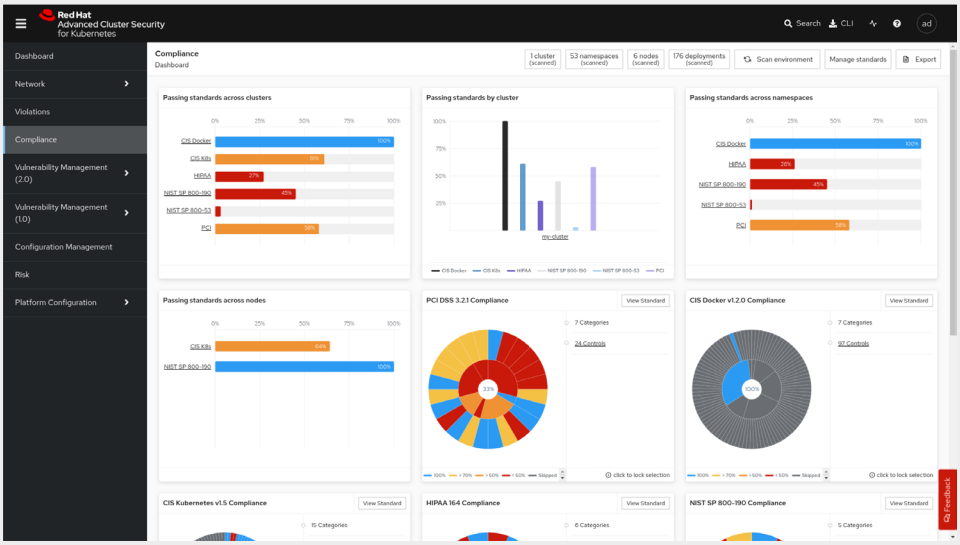

図 7. コンプライアンスの概要

4.4.1 - ランタイムソフトウェア内の脆弱性

コンテナランタイムの脆弱性を注意深く監視して、問題が検出された場合は迅速に修復する必要があります。

ソリューション

Red Hat Advanced Cluster Security：

1. Red Hat Enterprise Linux® CoreOS ノードの脆弱性をスキャンし、潜在的なセキュリティ脅威を検出します。
2. ランタイムソフトウェアのスキャンが含まれます。

OpenShift Container Platform：

- 環境全体が最新の状態に保たれるように、利用可能なアップグレードについて、ダッシュボードにアラートが表示されます。

Red Hat Advanced Cluster Management：

1. 非準拠となっているクラスタを適切に分離するために、マルチクラスタをタグベースで整理します。
2. サードパーティとの複数の統合を備えたアラートシステムを備えています。

4.4.2 - コンテナからの無制限ネットワークアクセス

コンテナからのアウトバウンド・ネットワークトラフィックの制御を実装します。さまざまな機密レベルのネットワーク全体でトラフィックが送信されるのを防ぎます。

ソリューション

Red Hat Advanced Cluster Security：

1. Kubernetes ネットワーク・セグメンテーションルールがすべてのデプロイメントに適用されているかどうかのチェックを実行します。
2. ネットワークトポロジを理解できるように、既存のネットワーク接続の視覚的なシミュレーションを提供します。ネットワークグラフは、許可されたアクティブな接続を識別し、アプリケーション間のセグメンテーション・ポリシーのギャップを特定するのに役立ちます。
3. オンデマンドのネットワークポリシー (YAML ファイル) を生成し、それを Kubernetes デプロイメントにプッシュして、ネットワーク・セキュリティポスチャを強化します。

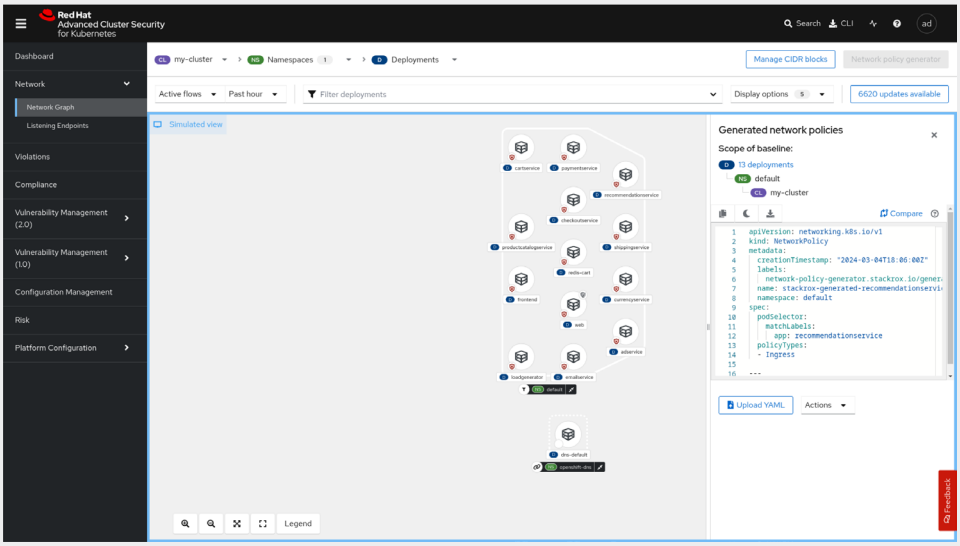

図 8. ネットワークポリシー・ジェネレーター

4.4.3 - セキュアでないコンテナランタイムの設定

Center for Internet Security (CIS) Docker Benchmark などのコンテナランタイム構成標準への準拠を自動化し、環境全体の構成設定を継続的に評価します。

ソリューション

Red Hat Advanced Cluster Security：

- 環境をスキャンし、CIS Docker および Kubernetes ベンチマークに対してコンプライアンスチェックを実行して、コンテナ環境全体で継続的にコンプライアンスを確保します。

さらに、次のようなすぐに使用できるコンプライアンスポリシーがあります。

1. Payment Card Industry Data Security Standard (PCI-DSS)
2. Health Insurance Portability and Accountability Act (HIPAA)

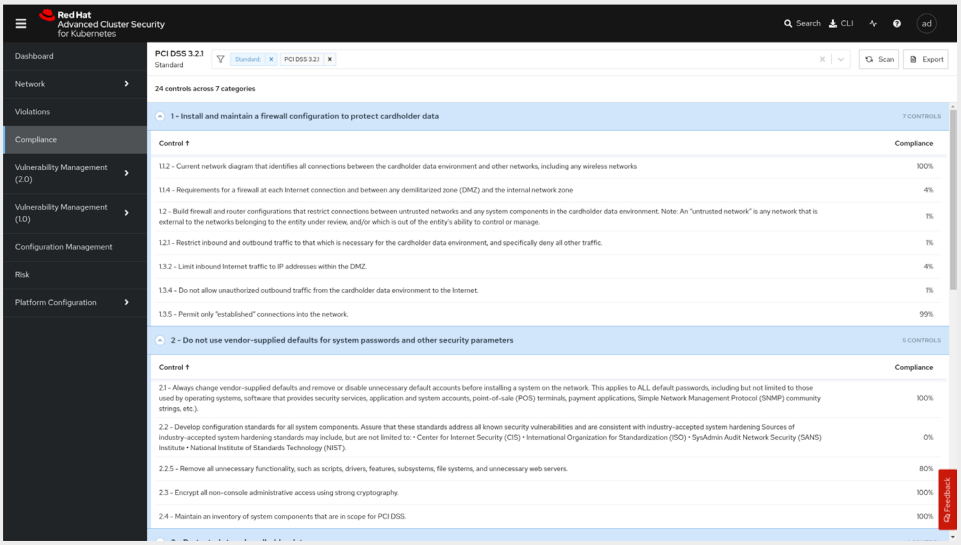

図 9. PCI DSS コンプライアンス標準の結果

4.4.4 - アプリケーションの脆弱性

コンテナやコンテナ・インフラストラクチャへの侵入などの脅威を検出することを目的としたセキュリティ制御を実装します。

ソリューション

Red Hat Advanced Cluster Security：

動作モデリングとルールおよびホワイトリストを組み合わせて、予期しないアクティビティを含むコンテナに対する脅威を検出します。以下はその例です。

1. すぐに使えるポリシーにより、ファイル名とパスに基づいてパッケージマネージャーの使用と不審なプロセスの実行を検出します。
2. オンデマンドスキャンにより、重要なシステムファイルの変更など、ホスト上の変更につながる可能性のある危険な構成を特定します。

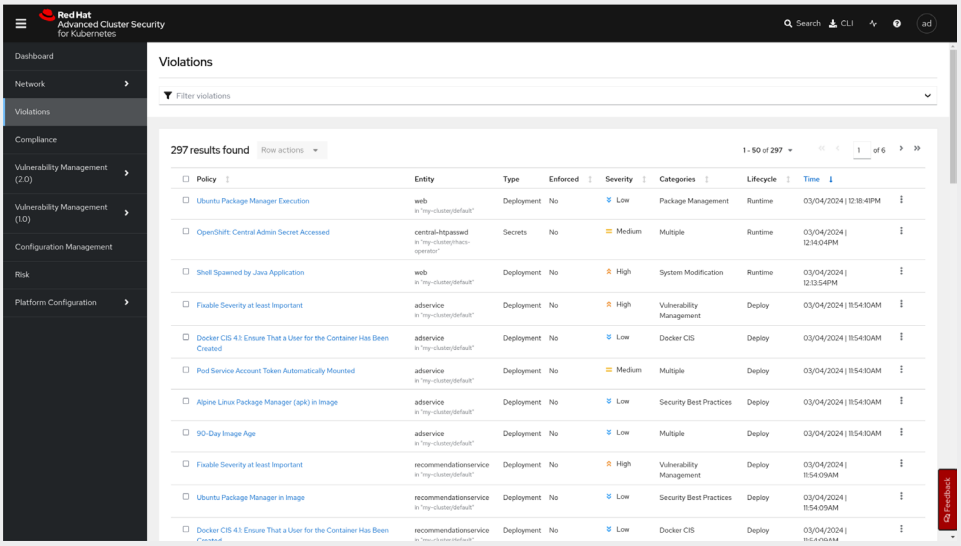

図 10. 違反ダッシュボード

4.5.1 - 大きなアタックサーフェス

可能な場合は、コンテナ固有のオペレーティングシステム (OS) を使用します。コンテナをホストするために特別に設計された OS は通常、デフォルトで強化されているからです。コンテナ固有の OS を使用できない場合は、ホスト OS を強化して攻撃対象領域を減らします。

ソリューション

Red Hat Advanced Cluster Security：

1. CoreOS や Google Container Optimized OS など、コンテナ固有の OS の使用をサポートします。
2. クラスタにデプロイされたノード OS を識別し、コンプライアンスの証拠として CoreOS や Google Container-Optimized OS などのコンテナ固有の OS の使用を検証します。
3. CIS General Linux ベンチマークに準拠し、強化されたセキュリティで Linux ホストが構成されていることを確認できます。
4. コンテナ固有の OS が使用されていないインスタンスでも、CIS Docker および Kubernetes ベンチマークに準拠して環境が強化されていることを確認できます。

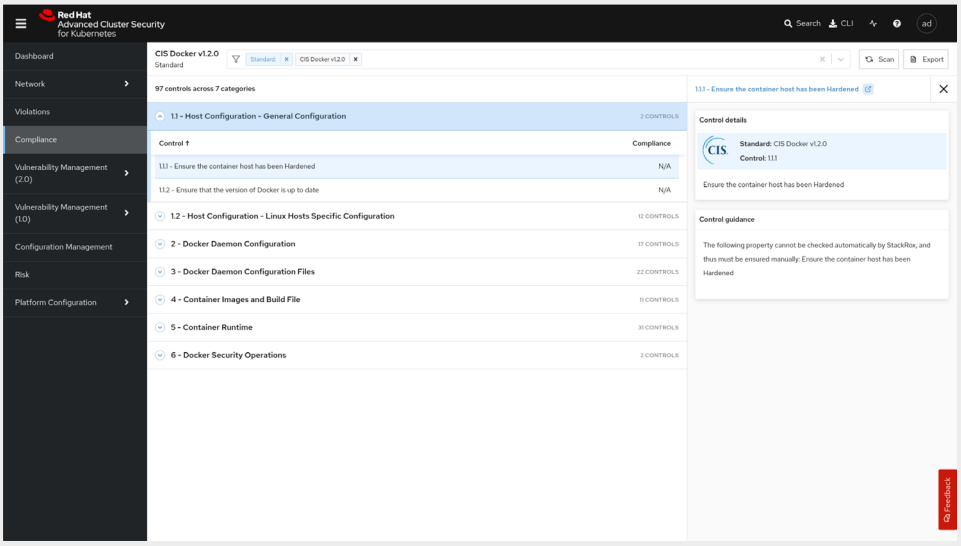

図 11. CIS Docker コンプライアンス標準の結果

4.5.2 - 共有カーネル

組織は、同じホストインスタンス上で、コンテナ化されたワークロードとコンテナ化されていないワークロードを混在させないようにする必要があります。

ソリューション

OpenShift Container Platform：

- サポートされているインストールは、Red Hat OpenShift がホスト上の唯一のワークロードであるインストールです。サポートできるようにするには、OpenShift Container Platform と同じホスト上で他のワークロードを実行しないようにする必要があります。

4.5.3 - ホスト OS コンポーネントの脆弱性

組織は、基本 OS の管理および機能向けに提供されるコンポーネントのバージョン管理を検証するための管理プラクティスとツールを実装する必要があります。

ソリューション

Red Hat Advanced Cluster Security：

- Red Hat CoreOS ノードの脆弱性をスキャンし、潜在的なセキュリティ脅威を検出できます。Red Hat Advanced Cluster Security は、Red Hat CoreOS インストールの一部としてノードホストにインストールされている Red Hat CoreOS RPM をスキャンし、既知の脆弱性を検出します。

4.5.4 - 不適切なユーザーアクセス権

組織は引き続き、OS に対するすべての認証の監査、ログイン異常の監視、特権操作を実行するためのエスカレーションのログへの記録が確実に行われるようにする必要があります。

ソリューション

OpenShift Container Platform：

- ホスト OS へのアクセスを制限します。ホスト OS にアクセスする推奨方法は、oc debug コマンドを使用することです。

Red Hat Advanced Cluster Security：

- デバッグポッドの実行中にプロセスを監視できます。ポリシーを作成して、privileged=true などのアノテーションを含むポッドを監視することもできます。

4.5.5 - ホストファイルシステムの改ざん

コンテナが必要な最小限のファイルシステム権限セットで実行されていることを確認します。

ソリューション

Red Hat Advanced Cluster Security：

すべてのデプロイメントでマウントされているボリュームを分析し、基盤となるホストファイルシステムのファイルまたはディレクトリがデプロイメントでマウントされているかどうかを検出します。これには以下が含まれます。

1. 機密性の高いホストパスをマウントするデプロイメントの検出、警告、またはブロック。
2. /var/run/docker.sock、/var/run/crio/crio.sock、および /run/crio/crio.sock の組み込みポリシーの提供。他のホストパスと一致するように構成できます。

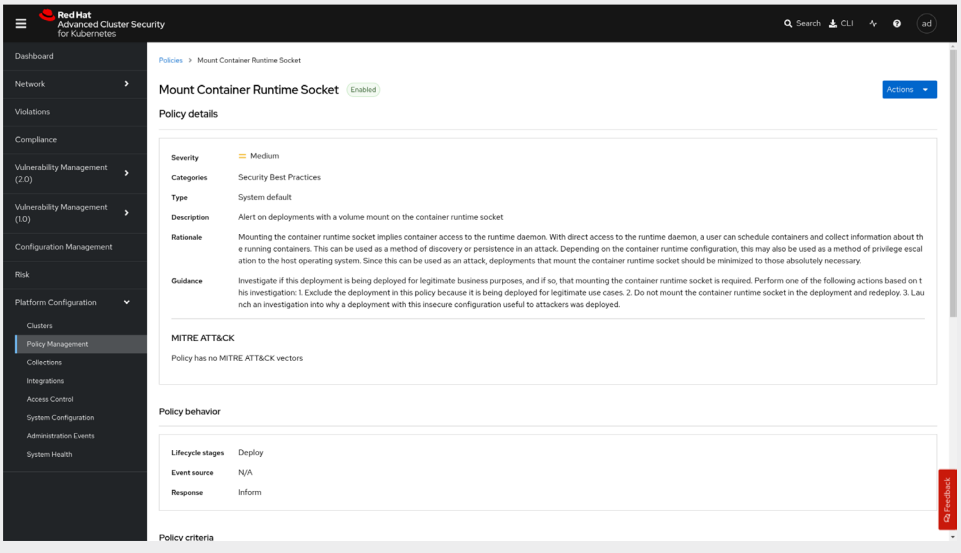

図 12. マウント・コンテナ・ランタイム・ソケットのポリシービュー

キーポイント

コンテナや Kubernetes など、クラウドネイティブ開発スタックのインフラストラクチャの変更によりセキュリティの状況が変化しており、その結果、NIST SP 800-190 のセキュリティプラクティスと標準規格を採用する必要性が高まっています。

ご使用の環境における NIST SP 800-190 コンプライアンスの状態を理解するために、Red Hat Advanced Cluster Security をお試しください。次のことを確認できます。

1. NIST SP 800-190 に基づく制御に対する、クラスタのセキュリティ全体の健全性。
2. 脆弱性と構成ミスといったリスクの高い組み合わせでデプロイされたサービス。
3. NIST SP 800-190 のコンプライアンス要件に影響を与える可能性がある CIS ベンチマークの失敗。
4. コンテナの攻撃対象領域全体での主要な脆弱性。
5. DevOps チームのベストプラクティスの構成。

エンタープライズ・デプロイメントの場合は、OpenShift Container Platform、Red Hat Advanced Cluster Security、Red Hat Advanced Cluster Management、Red Hat Data Foundations、および Quay を含む OpenShift Platform Plus に投資することを強くお勧めします。これらの製品を使用することで、NIST SP 800-190 に準拠するための主要なリスクポイントを遵守できます。

その他の情報：Red Hat を使用した Kubernetes ネイティブセキュリティの実装

Kubernetes を保護するために設計されたセキュリティ・プラットフォームにより、強力なセキュリティと運用上の利点を実現します。Kubernetes ネイティブのセキュリティは、Kubernetes レイヤーで制御を適用し、一貫性、自動化、拡張性を確保します。組織はセキュリティをコードとして導入し、セキュリティを後付けするのではなく、最初から組み込むことができます。

こちらのホワイトペーパー『Kubernetes-native Security: what is it and why it matters』をダウンロードして、Kubernetes ネイティブセキュリティの主な機能と利点についてご覧いただき、既存のコンテナセキュリティ・アプローチと Kubernetes 環境専用の保護を提供するというアプローチの違いについてご確認ください。

Red Hat について

エンタープライズ・オープンソース・ソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、クラウドネイティブ・アプリケーションの開発、既存および新規 IT アプリケーションの統合、複雑な環境の自動化および運用管理を支援します。受賞歴のあるサポート、トレーニング、コンサルティングサービスを提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーであり、オープンな技術革新によるメリットをあらゆる業界に提供します。Red Hat は企業、パートナー、およびコミュニティのグローバルネットワークの中核として、企業の成長と変革を支え、デジタル化が進む将来に備える支援を提供しています。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#1156544_0524