sysdig

イメージスキャンに関するベストプラクティス5選

アプリケーションデリバリーを減速させることなく、コンテナのセキュリティリスクを管理するにはどうすればよいでしょうか？

この課題に対処する1つの方法として、イメージスキャンという、コンテナイメージの内容とビルドプロセスを分析し、セキュリティ上の問題、脆弱性、および不適切な処理を検出するプロセスがあります。イメージスキャンを DevOps ワークフローに組み込むことで、脆弱性が悪用される前に検知してブロックする第一の防御策として機能させることができます。

この文書では、セキュリティを自社ワークフローにシームレスに組み込むのに役立つ、効果的なコンテナイメージスキャン戦略を採用するためのベストプラクティスを5つ紹介します。

01

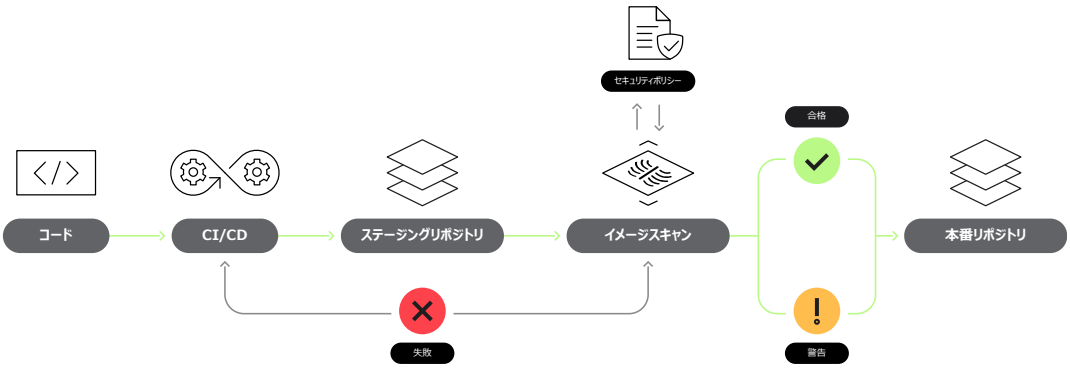
イメージスキャンを自社のCI/CDパイプラインに組み込むこと

コンテナイメージを構築する際には、公開前にそれらを必ずスキャンする必要があります。

DevOpsワークフロー向けにすでに構築中のCI/CDパイプラインに、イメージスキャンのための追加ステップを加えることができます。

CI/CDパイプラインにおけるイメージスキャンの基本は次の通りです。コードがテストされビルドされた後、本番環境のリポジトリにイメージをプッシュする代わりに、ステージングリポジトリにイメージをプッシュします。その後、イメージスキャンツールを実行します。これらのツールは通常、発見されたさまざまな問題をリストアップした上で、それぞれの問題に異なる深刻度を割り当てたレポートを返します。CI/CDパイプラインでこれらのイメージスキャン結果を確認し、重大な問題がある場合はビルドを停止することができます。CI/CDパイプラインでこれらのイメージスキャン結果を確認し、重大な問題がある場合はビルドを停止することができます。

ここでは自動化が鍵であることを忘れないでください。CI/CDパイプラインにセキュリティを組み込むことで、レジストリに侵入する前に脆弱性を検知でき、問題が本番環境に影響を及ぼすことはありません。



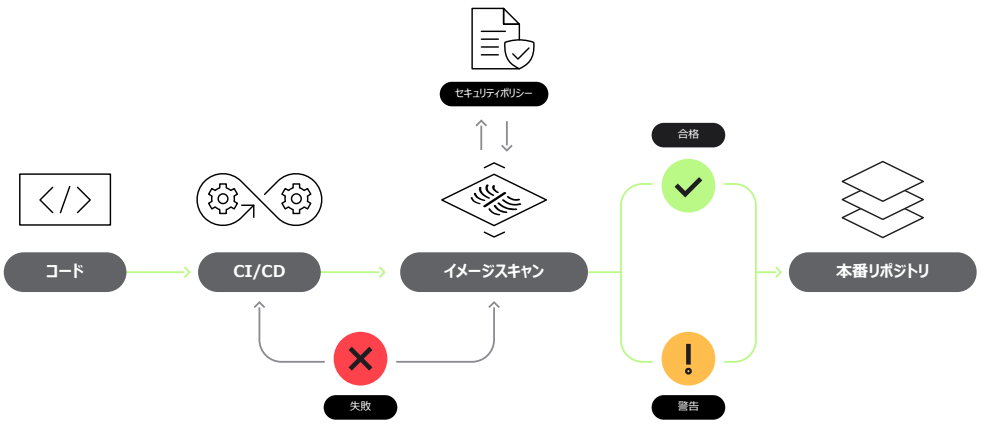
02

自社のプライバシーを管理するためにインラインスキャンを採用すること

従来、CI/CDパイプラインでのイメージスキャンにはステージングリポジトリが必要でした。しかし、もしイメージに誤って認証情報が含まれていたとしたらどうでしょう？それらの認証情報が攻撃者の手に渡り、流出してしまう可能性があります。

さらに一歩進んで、インラインイメージスキャンを実装することができます。インラインイメージスキャンとは、ステージングリポジトリを必要とせずに、CI/CDパイプラインから直接イメージをスキャンするものです。

スキャンのメタデータのみがスキャンツールに送信されるため、プライバシーを管理できるようになります。

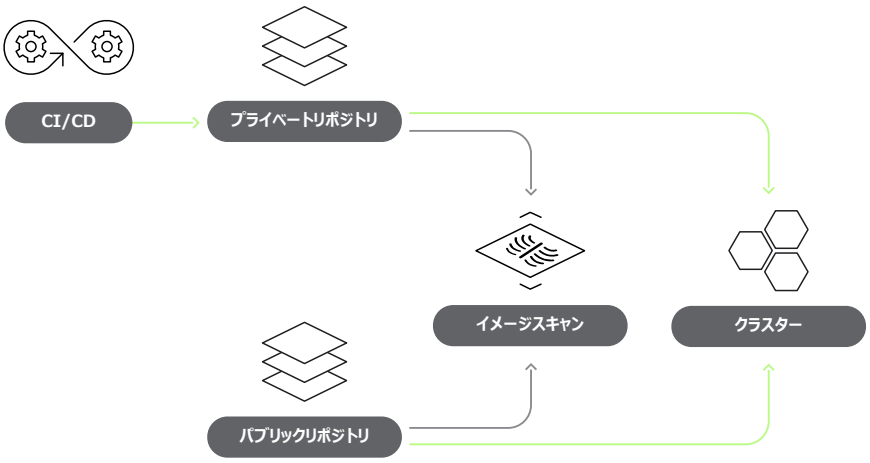


03

お使いのコンテナレジストリ内にあるイメージを定期的にスキャンすること

コンテナレジストリ内にあるイメージを定期的にスキャンすることで、過去にスキャン済みのイメージに影響を与えるような新たな脆弱性を特定できるようになります。

レジストリからイメージをプルするため、お客様自身がイメージを定期的にスキャンすることが重要となります。これにより、イメージがレジストリにチェックインされた後に発生する可能性のあるセキュリティリスクを特定できるようになります。

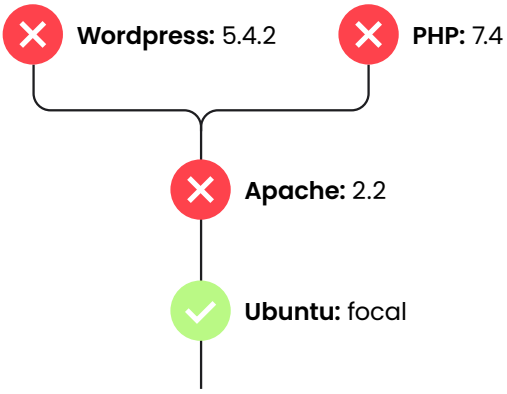


04

OSの脆弱性をスキャンすること

一般的に、イメージは軽ければ軽いほどより望ましいものとなります。なぜなら、イメージが軽いほど、ビルドがより速くなり、スキャンがより速くなり、かつ潜在的な脆弱性を含む依存関係が少なくなることを意味するからです。

新規のDockerイメージは、通常、既存のベースイメージを基に構築されます。このベースイメージは、イメージのDockerfileのFROMステートメントで定義されます。その結果、最も一般的なタスクにおいて多くの時間を節約できるような階層型のアーキテクチャー設計を実現できます。例えば、イメージのスキャンに関しては、ベースとなるイメージを一度スキャンするだけで十分です。親イメージに脆弱性がある場合、その上に構築された他のイメージにも脆弱性があります。



イメージに新たな脆弱性を導入しなかった場合であっても、ベースイメージに含まれている脆弱性の影響を受ける可能性はあります。

よって、お使いのスキャンツールが、既知の脆弱なイメージに関する脆弱性フィードを積極的に追跡する機能を持たなければならないのはこのためです。この機能により、影響を受けるイメージを使用している場合は、その旨を通知できるようになるからです。

05

サードパーティ製ライブラリに含まれている脆弱性をスキャンすること

アプリケーションは多くのライブラリを使用します。このため、ライブラリを利用すると、社内チームが実際に書くコードよりも多くの行数のコードが追加されてしまいます。これは、自社で書いたコードだけではなく、そのコードが持つ依存関係のすべてに脆弱性があることを認識しなければならないことを意味します。

幸運なことに、これらの脆弱性は、スキャナがOSの脆弱性について警告するのと同じように、脆弱性フィードにおいてきちんと追跡されています。すべてのツールが、イメージ内のライブラリをスキャンするほど深く掘り下げるわけではありません。お使いのイメージスキャナが十分に深く掘り下げを行い、これらの脆弱性について警告することを確認してください。

イメージスキャンは、セキュアなDevOpsワークフローにおける最初の防御手段です。イメージスキャンに関するベストプラクティスに従うことで、アプリケーションデリバリーを減速させることなく、問題を引き起こす前に、検知できるようになります。

詳細については、当社のE-BOOK『**クラウドの保護：効果的な脆弱性管理へのガイド**』をご覧ください。

ダウンロードする ➡

PB-041-JA REV. A 3/25