Container Security - レジストリスキャン

Qualys Container Security を使用して、パブリックレジストリおよびプライベートレジストリをスキャンできます。パブリックレジストリは、Amazon、Azure、および Google でホストされるクラウドアクセスが可能なレジストリです。一方、プライベートレジストリは、Artifactory または Nexus を使用してホストされるレジストリなど、プライベートネットワークに配置されるオンプレミスのレジストリです。Qualys は、認証レジストリのスキャンのみサポートしています。

注記: Qualys Container Security では、現時点で、V2 タイプのレジストリのみスキャンできます。

レジストリをスキャンする方法

Qualys クラウドプラットフォームの Container Security アプリケーションから、センサイメージをダウンロードします。センサがレジストリおよび Qualys と通信できるネットワークに、(-r コマンドを使用して) センサをレジストリセンサとして配置します。

セキュリティ状態を得る必要があるリポジトリで、新しいレジストリを作成し、スキャンスケジュールを設定します。オンデマンドスキャンまたはスケジュールスキャンを実行できます。スケジュールスキャンは増分スキャンであるため、最終スキャン以降に設定リポジトリに追加される新規イメージのみが対象となります。

レジストリスキャンを設定する方法については、『Qualys Container Security User Guide』を参照してください。

レジストリスキャンの動作

レジストリスキャンには、次の 2 つのフェーズがあります。
- 「Listing」フェーズ
- 「Scanning」フェーズ

「Listing」フェーズ

「Listing」フェーズでは、Container Security センサは、Docker Registry v2 API を呼び出して、レジストリのスキャンスケジュールで指定されたリポジトリのすべてのイメージメタデータ情報を収集します。
Qualys センサは、カタログ、タグ、マニフェストの作成、および設定 API 呼び出しを行って情報を収集します。この情報は UI に表示されます。 ユーザがスケジュールで定義したフィルタ (過去 14 日間に作成されたスキャンイメージなど) に基づいて、スキャンするイメージが実行待ちになります。

注記 - パブリックレジストリ (クラウドアクセスが可能) の場合、Qualys は Docker Registry API 呼び出しを行い、情報を取得して、イメージスキャンを実行できるようセンサに提供します。プライベートレジストリの場合、Qualys から接続することができないため、センサはリスト表示アクションとスキャンアクションの両方を実行し、Qualys に情報を提供します。

「Scanning」フェーズ

レジストリセンサとして準備されたセンサは、Qualys を定期的にポーリングして、スキャンを実行待ちのイメージがないか確認します。Qualys は、検出されたイメージのサブセットのみをスキャンするようセンサに割り当てます。応答ペイロードには、イメージの詳細と、レジストリからイメージを取得する際に必要な認証情報が含まれます。

無断複写・転載を禁じます。2019 年 クォリスジャパン株式会社

Qualys レジストリセンサは、これらのイメージをレジストリから取得し、情報（スナップショット）を Qualys クラウドに送信します。次に、Qualys は収集した情報への署名を実行し、脆弱性レポート
（Container Security UI で表示可能）を生成します。

レジストリにスキャン対象のイメージが多数ある場合、全体のスキャン時間は通常より長くかかります。複数のレジストリセンサをインストールして、スキャンのペイロードを分散することで、スキャンにかかる時間と結果表示にかかる時間を短縮できます。

最終更新日: 2019 年 1 月 14 日