アクション計画とマイルストーン

アクション計画とマイルストーンの概要

Cisco vMonitor は、潜在的な問題について官公庁向け Cisco SD-WAN を継続的にスキャンします。Cisco vMonitor は、収集されたデータを処理し、潜在的な脆弱性に関するアクション計画とマイルストーン（POA&M）アラートを作成します。各 POA&M アラートでは JIRA チケットが生成されます。

Cisco FedOps ユーザーは、Cisco SD-WAN セルフサービスポータル で POA&M レポートを表示およびダウンロードすることができます。これは、ユーザーが連邦政府 IdP 経由でログインしているかどうかを確認することによって可能になります。Cisco FedOps は、ロールに関係なく、POA&M レポートにアクセスできます。これらのレポートを使用することで、官公庁向け Cisco SD-WAN 環境をモニタリングし、潜在的なリスクと問題を特定することができます。

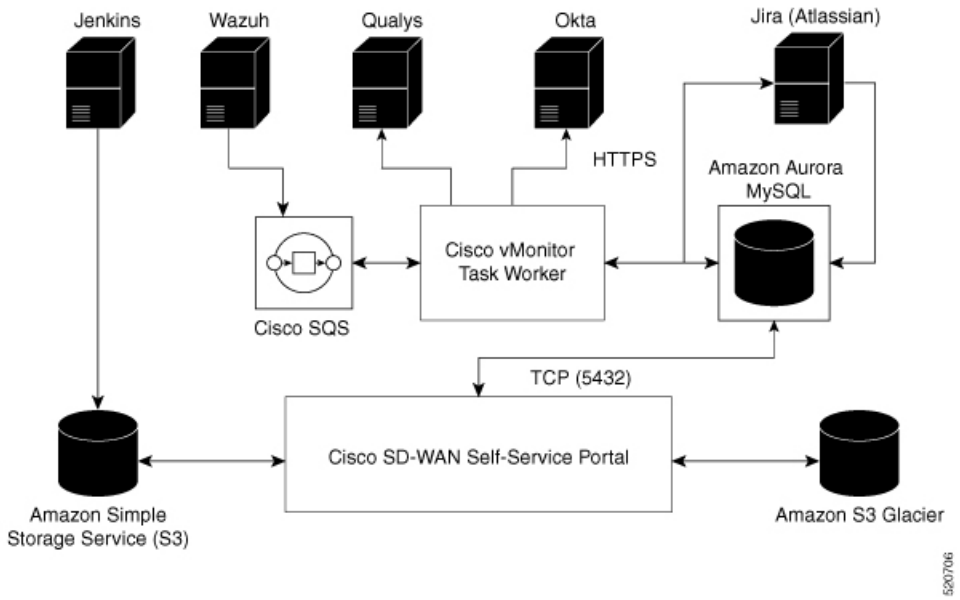
官公庁向け Cisco SD-WAN は、分散型モデルを使用して、次のソースからデータを収集します。

- Okta：Okta ログイベント
- Wazuh：標準 Wazuh スキャン
- Qualys：脆弱性アラートとコンプライアンスアラート

アクション計画とマイルストーンのアラートを作成するための Cisco vMonitor のプロセス

次の図は、Cisco vMonitor が収集された脆弱性データを処理して POA&M アラートを作成する方法を示しています。

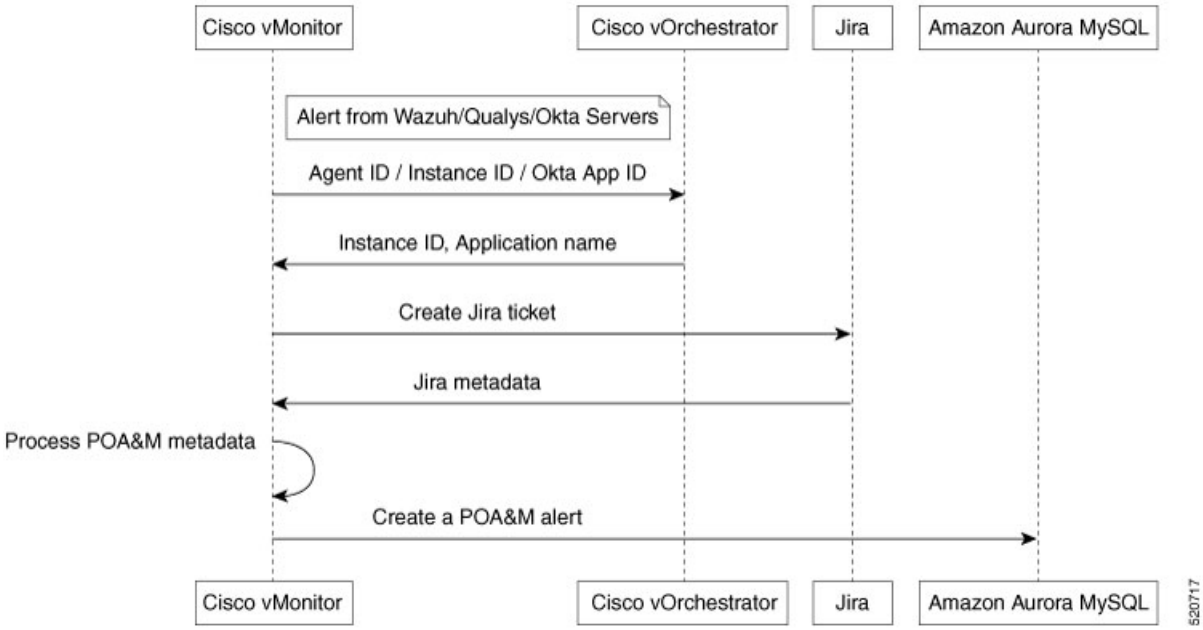
図 *1 : POA&M* アラートを作成するための *Cisco vMonitor* のプロセス



アクション計画とマイルストーンのアラートを生成するワークフロー

Cisco vMonitor では、次の図に示すワークフローを実行することにより、タスクワーカーを使用して POA&M 脆弱性アラートが作成されます。

図 *2 : POA&M* アラートを生成するワークフロー



Cisco vMonitor は次のアクションを実行します。

1. さまざまなデータソースからログを収集します。

   - Okta：Cisco vMonitor は、RESTful API を使用して、警告ログとエラーログ（重大度が ERROR または WARN）をフィルタ処理します。また、Cisco vMonitor は、これらのログを Okta サーバーから定期的に取得します。1 回のコールで、Cisco vMonitor は最大 500 のイベントを取得します。500 を超えるイベントが存在する場合、イベントはバッチで取得されます。
   - Qualys：Cisco vMonitor は、アラートデータを定期的に取得します。
   - Wazuh：このサーバーは、アラートデータを Amazon Simple Queue Service（SQS）に送信します。Cisco vMonitor は、SQS からデータを定期的に取得します。

2. Cisco vOrchestrator からのログとデータを関連付けて、POA&M アラートを作成します。

   - Qualys：Cisco vMonitor は、インスタンス ID をキーとして使用して、Cisco vOrchestrator のアプリケーションテーブルからアプリケーション名とアプリケーションバージョンを検索します。
   - Wazuh：Cisco vMonitor は、Wazuh エージェント ID をキーとして使用して、Cisco vOrchestrator のアプリケーションテーブルからアプリケーション名とアプリケーションバージョンを検索します。
   - Okta：Cisco vMonitor は、Okta アプリケーションターゲット ID をキーとして使用して、Cisco vOrchestrator のアプリケーションテーブルからアプリケーション名とアプリケーションバージョンを検索します。

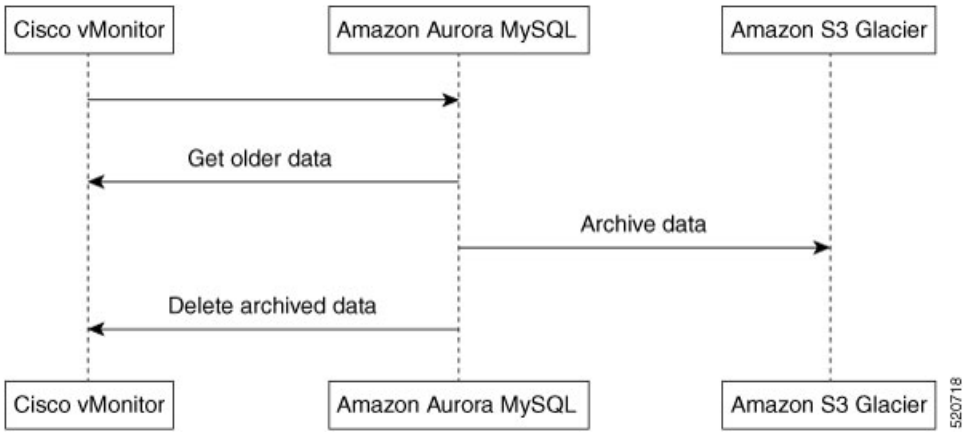
3. 次のトラッカーを作成または更新します。
   - JIRA チケット：Cisco FedOps が問題を追跡して対処するために使用します。
   - POA&M アラート：計算されたすべてのメタデータを使用してアラートが生成され、Amazon Aurora データベースの POAM テーブルに保存されます（Cisco SD-WAN SSP は、このデータベースを使用して POA&M アラートを生成します）。

データ消去

過去 180 日間のデータは Amazon Aurora データベースに保存されており、すぐに取得できます（Cisco SD-WAN SSP には過去 30 日間のアラートが表示されます）。

180 日以上前のアラートは、Amazon S3 Glacier を使用してアーカイブされます。夜ごとにジョブが実行され、その後、長期保存のためにデータが Amazon S3 Glacier に移動されます。180 日以上前のデータについては、Cisco SD-WAN SSP での日付範囲のものにアクセスできます。

図 *3:* データ消去のワークフロー



アクション計画とマイルストーンの表示

POA&M レポートを表示するには、次の手順に従います。

1. Cisco SD-WAN SSP ダッシュボードで、[Regulatored] をクリックします。

   オーバーレイネットワークの脆弱性フィードを提供する [POAM] ウィンドウが表示されます。Qualys、Wazuh などのソースを使用すると、[POAM] ウィンドウにさまざまな問題が一覧表示されます。このレポートを検索、分類、およびダウンロードできます。ダウンロードしたレポートは、Splunk などのセキュリティ情報イベント管理（SIEM）ソフトウェアに提供できます。

2. [POAM] ウィンドウで、次のタスクを実行します。

- 検索バーを使用して、問題をフィルタリングおよび検索します。POAM ステータス、リスク評価、問題検出のカスタム日付範囲といったさまざまなパラメータでフィルタリングできます。
- 特定の問題に関する情報を表示するには、[Details] をクリックします。

  アラートに関する追加情報（問題の説明など）を示すダイアログボックスが表示されます。
- 特定の列でフィルタリングするには、列の下にあるテキストボックスをクリックします。たとえば、[Adjusted Risk] 列の下をクリックし、「**high**」と入力すると、すべての高リスク問題を一覧表示できます。