Setup Integration from Qualys

Qualys VMDR Integration Guide

Integrate **Qualys Vulnerability Management, Detection and Response (VMDR)** with the Elastic Stack via REST API to ingest vulnerability, asset, and detection data directly into Elasticsearch for centralized security monitoring and analysis.

Credentials & API Access Setup

Before configuring the integration, you'll need to prepare your API credentials in Qualys:

Steps:

1. Log in to the **Qualys Admin Portal**.
2. Go to **User Management**.
3. Create or select a dedicated **API User** with:
   - **API Access permission**
   - Access to:
     - **VMDR Module**
     - **Host Detection**
     - **Asset Inventory**
     - **Knowledge Base**
     - **User Activity Log** (if required)
4. Take note of:
   - **Username**
   - **Password**
   - Your **Qualys Platform API URL**:
     - Check via: Qualys Platform Identification
     - Or log in to Qualys → Help → About → see "Security Operations Center (SOC)" for your URL.

Elastic Integration Configuration

In Kibana:

1. Go to **Management → Integrations**.

2. In the search bar, type **Qualys VMDR**.
3. Select **Qualys VMDR** from the search results.
4. Click **Add Qualys VMDR Integration**.

Provide the following connection details based on the data you want to collect:

Data Stream	Required Details
Asset Host Detection	username, password, API URL, interval, input parameters, batch size
Knowledge Base	username, password, API URL, initial interval, interval, input parameters
User Activity Log	username, password, API URL, initial interval, interval

5. Save the integration.

Permissions Reference (API User)

Data Stream	Role	Permission Scope
Asset Host Detection	Managers, Unit Managers, Scanners, Readers	VM scanned hosts (depending on role scope)
Knowledge Base	Managers, Unit Managers, Scanners, Readers	Can download vulnerability data
User Activity Log	Managers, Unit Managers, Scanners, Readers	Can view user actions (own or others, depending on role)

Revision #4
Created 19 June 2025 07:26:59
Updated 11 July 2025 16:58:17