Mandiant

CROWDSTRIKE INTEL

API Calls

The CrowdStrike API is used by the Validation Platform to bring in the Threat Actor information. Both the OAuth2 and legacy CrowdStrike API key are supported in the CrowdStrike integration.

Purpose	Call
Threat Actor List Query	/actors/queries/actors/v1
Threat Actor Details Query	/actors/entities/actors/v1?ids={actor_id}
Threat Actor Malware Families	/indicator/v2/search/?actor.match={actor_name}

Prerequisites

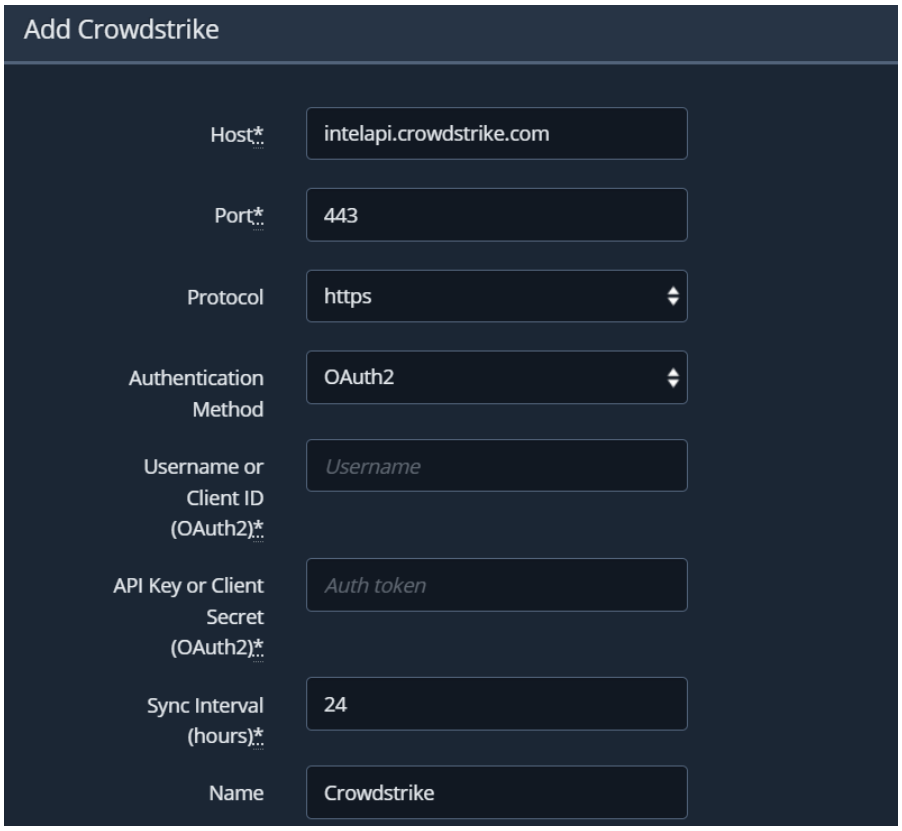
Information to gather before you start:

- Identify the host, port, and protocol.
- Identify the username and authentication token. Any account that has API access can be used. That account must have the following API permissions:
  - Read: Actors (Falcon X)
  - Read: IOCs (Indicators of Compromise)

Configuration

TO ADD THE CROWDSTRIKE THREAT INTELLIGENCE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **Crowdstrike**.
3. Enter the **Host**.
4. Enter the **Port**.
5. Select the **Protocol**.
6. Select the **Authentication Method**.
7. Enter the Username or Client ID.
   - If you are using Legacy API Key, enter the Username.
   - If you are using OAuth2, enter the Client ID.
8. Enter the API Key or Client Secret.
   - If you are using Legacy API Key, enter the API Key.
   - If you are using OAuth2, enter the Client Secret.
9. Enter the **Sync Interval** in hours (default: 24 hours).
10. (Optional) Assign a **Name**.
11. Click **Submit**. The integration automatically starts to sync after it is added.



Add Crowdstrike Intel Integration

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.