CrowdStrike and WitFoo
Integration Configuration Guide

Partner Product:

WitFoo Precinct version 2017.08.25.1 and greater

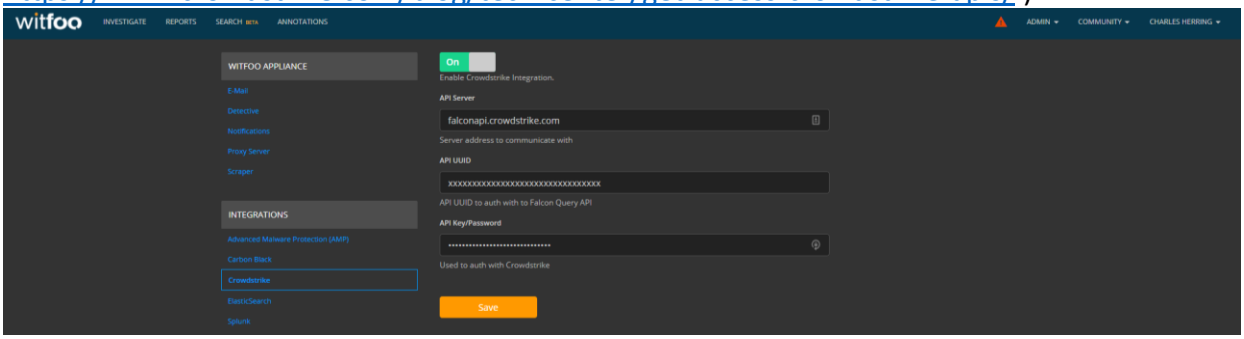
Overview

WitFoo Precinct leverages the Falcon Query API to import and process Crowdstrike detections. The data from these detections & underlying assets are utilized to create and enhance WitFoo incidents.

Configuration and Setup:

Step 1: Login to WitFoo Precinct. Go to Admin -> Settings -> Crowdstrike

Step 2: Turn on the integration and provide Falcon Query API credentials (see: https://www.crowdstrike.com/blog/tech-center/get-access-crowdstrike-apis/.)



Step 3: Hit “Save” and verify a Checkmark is displayed next to Save.

Step 4: The initial processing may take up to 10 minutes. Once complete, Crowdstrike enhanced incidents will appear on the “Investigate” tab and in Leads under “Search”

CROWDSTRIKE