

CrowdStrike and WitFoo Integration Configuration Guide

Partner Product:

WitFoo Precinct version 2017.08.25.1 and greater

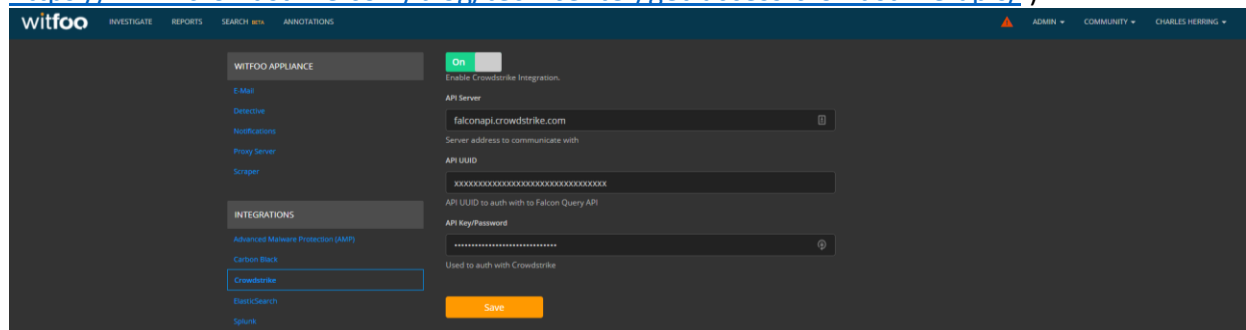
Overview

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/.](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

The screenshot displays the CrowdStrike Witfo interface for investigating a host. The main area shows a network diagram with a central host node 'M2401803.asi' (yellow) connected to several other nodes: 'powershell.exe' (two instances) and 'regsvr32.exe'. The interface includes a sidebar with incident filters, a top navigation bar, and a right-hand panel with host details and evidence.

Incidents Sidebar:

- Search Term: Host, Cmd, or File Name
- Search: [Button]
- Incident Activity: Today (2), Last 7 Days (8), Last 30 Days (8), All (8)
- Suspicion Score: 0.00-0.24 (1), 0.75-0.99 (7)
- Lead Types: Exploiting Host (8), Staging Host (8), Exfiltration Host (4), Suspicious User (2), Exploiting Target (8), Staging Target (8), Exfiltration Target (5), C2 Server (3), Bot (3), Malicious File (2)
- Status: Open Cases (7), Confirmed Cases (1), Acquired Cases (1)

Host Details Panel:

- Host Name: M2401803
- IP: 192.168.1.100
- Network: Internal
- MAC Address: [Redacted]
- Host is in the internal network.
- EVIDENCE: Reputation Score: 0.85 (Infectious: +0.85, Hostile: -0.00); Lab Results: Crowdstrike Detection (Infectious: +0.85, Hostile: -0.00); Lead Type(s): Exploiting Host (Witfo): 2017-09-05 18:21:04
- ASSOCIATED HOSTNAMES: [None]
- RELATED INCIDENTS: [None]
- ANNOTATIONS: [None]
- [Annotate Button]

Leads Table:

Observed Time	Reporting Tool	Event Type	Details	Status
2017-09-05 06:21:00 UTC	CrowdStrike	CrowdStrike Malware Detection	CrowdStrike Malware Detection	Open
2017-09-05 06:21:00 UTC	Witfo Labs	Witfo Lab Match	CrowdStrike Detection confirmed	Open
2017-09-05 06:20:59 UTC	CrowdStrike	CrowdStrike Malware Detection	CrowdStrike Malware Detection	Open