ThreatConnect & Crowdstrike Falcon Host

Through an expanded partnership with **CrowdStrike**, **ThreatConnect®** users can now act on intelligence in CrowdStrike Falcon Host.

This integration allows users to discover and investigate both current and historic endpoint activity within seconds of ThreatConnect sending an indicator to CrowdStrike Falcon Host.

The Challenge

Cybersecurity teams don't have enough context about their threat data, making it difficult to decide where to focus their efforts.

Many security tools are focused on detecting malware, but attackers now utilize numerous techniques that go beyond malware, such as privilege escalation and zero-day exploits. In order to protect your network, you need more information about your indicators so you know how to adequately block them.

The Solution

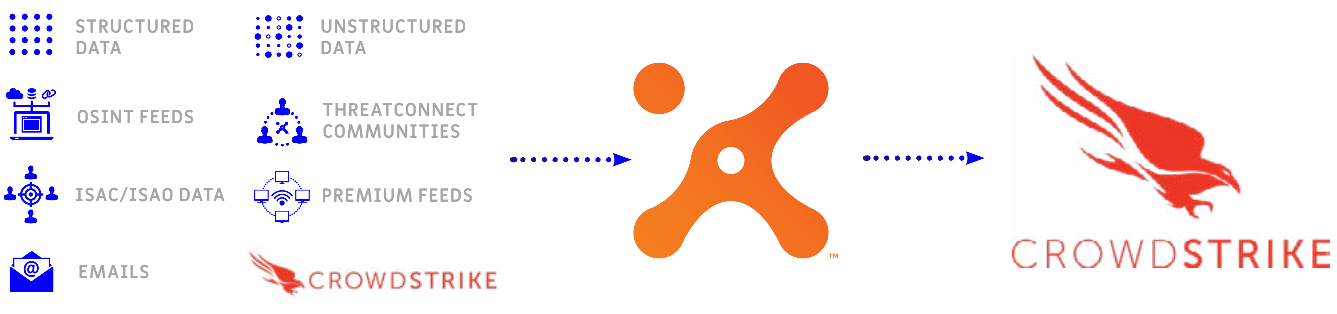
The ThreatConnect and CrowdStrike Falcon Host integration:

- ✓ Provides ThreatConnect users the ability to send all indicators, including third-party IOC's to CrowdStrike Falcon Host for alerting
- ✓ Allows indicator filtering, giving users full control of which ThreatConnect indicators are sent to CrowdStrike
- ✓ Ensures users are working with the most relevant data for their organization
- ✓ Grants full visibility into current and historic endpoint activity, so you can identify exactly which endpoints are vulnerable to specific indicators

Ingest threat data from multiple sources

Correlate, normalize, and enrich threat data in ThreatConnect

Send validated IDS or IPS to your firewall for alerting and blocking



ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Features & Benefits

- ✓ Sends indicators from ThreatConnect to CrowdStrike Falcon Host for alerting
- ✓ Instantly shows endpoint activity, both current and historic
- ✓ Users have full control of which ThreatConnect indicators are sent to CrowdStrike Falcon Host

How to Get Started

If you already have an account with ThreatConnect, contact your Customer Success Engineer for information on how to integrate with Crowdstrike Falcon Host.

If you want to get access to the ThreatConnect and CrowdStrike integration, please contact **sales@threatconnect.com or 800.965.2708.**

CROWDSTRIKE

ABOUT CROWDSTRIKE

CrowdStrikeTM is a cybersecurity technology firm pioneering cloud delivered next-generation endpoint protection and services. The CrowdStrike Falcon platform stops breaches by preventing, detecting and responding to all attacks types, at every stage – even malware-free intrusions.

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708