CROWDSTRIKE

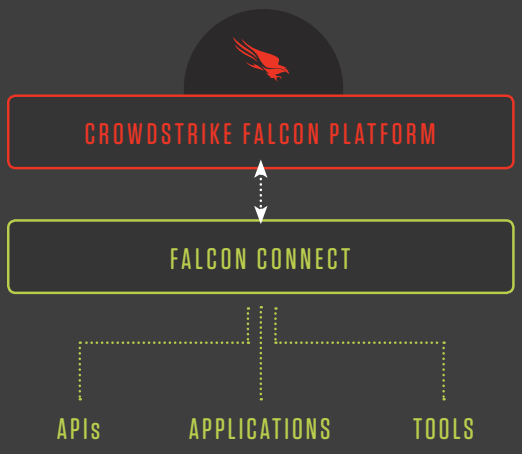
FALCON CONNECT

Powerful integration with the Falcon Platform

Falcon Connect provides a rich set of resources, including APIs (Application Programming Interfaces), applications and tools needed to develop, integrate and extend the use of the Falcon Platform into existing security solutions.

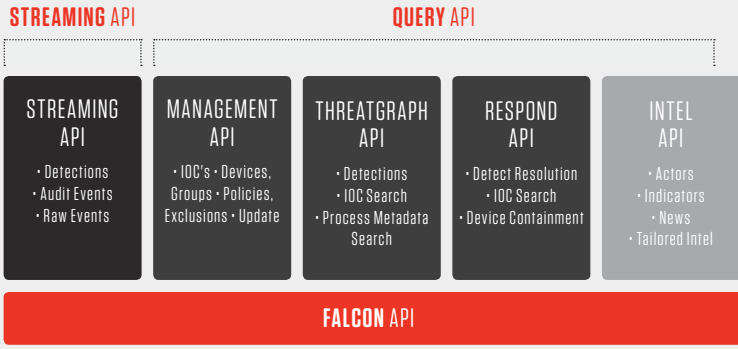
HARNESSING AND EXTENDING THE POWER OF THE FALCON PLATFORM

Falcon Connect makes the the Falcon Platform open and extensible by allowing customers and partners to easily integrate with CrowdStrike. It's purpose is to enable the CrowdStrike community to grow stronger by fully leveraging the power of the CrowdStrike Falcon Platform.



APIs

The Falcon APIs allow customers to fully take advantage of their existing security tools and to build automated solutions. A broad set of sophisticated and easy-to-use APIs is available for applications to connect with the Falcon Platform and other external data sources.



THERE ARE FIVE MAIN APIs CATEGORIES.

- **Falcon Streaming API** - streams detection and raw event data in near real-time.
- **Falcon Management API** - provides IOCs (Indicators of Compromise) and policy management, and additional device details.
- **CrowdStrike Threat Graph™** API - enables customers to query and traverse the CrowdStrike ThreatGraph to enable powerful visualization and hunting capabilities.
- **Falcon Respond API** - provides functionality to manage detections and enact remediation efforts
- **Falcon Intelligence API** - provides a feed of information, spanning adversary actors, indicators and news.

APPLICATIONS

Falcon Connect provides a rich environment to develop and deliver compelling and powerful applications that help security professionals and teams unleash the power of the Falcon Platform. Falcon Orchestrator and Falcon SIEM Connector are applications developed using Falcon Connect, and are available to the CrowdStrike community.

FALCON ORCHESTRATOR

Falcon Orchestrator provides enhanced workflow automation and remediation capabilities when used with Falcon Host. This application improves the overall effectiveness and efficiency of security and IT teams in conducting their security practices and operations in the areas of account containment, file extraction, remediation, asset monitoring and forensics.

- Integrates directly with Active Directory to retrieve metadata for user accounts involved in a Falcon Host detection event.
- Account containment: disable the account in Active Directory and enforce password reset with the click of a button.
- Integrates into SMTP environments to provide notifications, escalation and recurring reports.
- Open source application

Falcon SIEM Connector

The Falcon SIEM Connector streamlines and automates the process of gathering Falcon Host data, making it easier than ever for customers to leverage the power of Falcon Host in any SIEM or related system. The Falcon SIEM Connector automatically connects to the CrowdStrike Falcon Platform and normalizes the data into outputs that are immediately usable with SIEMs such as JSON, Syslog, CEF and LEEF.

Tools

CrowdStrike also provides tools and resources to enable customers, partners and developers to benefit from our technology and experience:

COMMUNITY TOOLS - a collection of resources ranging across vulnerability scanning, forensic collection, deobfuscation, and process inspection.

GITHUB REPOSITORY - a variety of scripts, source code, libraries and tools covering a variety of security and CrowdStrike-related areas.

RESOURCES

The Falcon Streaming and Query APIs and the Falcon SIEM Connector are downloadable from the Falcon Management Interface.

Falcon Orchestrator is available on Github at: https://github.com/CrowdStrike/

The Crowdstrike community tools can be downloaded at: www.crowdstrike.com/resources/community-tools/

LET'S DISCUSS YOUR NEEDS
Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services

Ver: 05-23-16