CROWDSTRIKE

CROWDSTRIKE FALCON APIs

HARNESSING AND EXTENDING THE POWER OF THE CROWDSTRIKE FALCON PLATFORM

The CrowdStrike Falcon® platform was designed to be open, with a focus on providing rich APIs to allow customers and partners to benefit from its power. The Falcon platform APIs access CrowdStrike cloud data, enabling you to leverage your existing security investments and enhance your protection.

Falcon platform APIs support both real-time streaming of endpoint data and security alerts, as well as on-demand queries of the Falcon Threat Graph™ database to support forensic and correlation efforts. Falcon Intelligence™ customers benefit from APIs that provide a feed of information spanning threat indicators, adversaries and intelligence reports.

KEY BENEFITS

» **Offers a comprehensive range of APIs**

» **Provides simple implementation and unrivaled ease-of-use**

» **Enables integration with other security solutions**

LEVERAGE THE POWER OF THE CROWDSTRIKE CLOUD

FALCON STREAMING API	FALCON DATA REPLICATOR API	FALCON QUERY API	FALCON INTEL API	FALCON THREAT GRAPH API
• Detections • Audit events	• Raw event data	• Search for IOCs, devices and detections • Manage detections and custom IOC watch list	• Actors • Indicators • News • Tailored intel	• Detections • IOC search • Process metadata
FALCON API				

PRODUCT OVERVIEW:

FALCON STREAMING API — STREAM DETECTION AND AUDIT EVENTS

The Falcon Streaming API allows you to receive real-time event and alerts from instances as they occur within a single data stream, providing a low-latency, high throughput delivery mechanism.

FALCON DATA REPLICATOR — EXPORT AND STORE ENDPOINT DATA IN YOUR ENVIRONMENT

The Falcon Data Replicator API allows Falcon Insight™ customers to export a copy of their endpoint data. It enables ingesting complete event data from the Falcon platform into your local data warehouse or data layer and correlating it against logs collected from other systems.

FALCON THREAT GRAPH API — ACCELERATE INVESTIGATION BY VISUALIZING RELATIONSHIPS

The Falcon Threat Graph API leverages CrowdStrike's multi-petabyte graph database to reveal the underlying relationships between indicators of compromise (IOCs), devices, processes and other forensic data and events such as files written, module loads or network connections. Integration with visualization tools enables you to traverse the graph of event data to investigate relationships between events.

FALCON QUERY API — MANAGE, INVESTIGATE AND RESPOND

The Falcon Query API allows you to upload IOCs for monitoring, obtain device information about systems with the Falcon agent installed, search for IOCs and related processes, and manage detection status.

FALCON INTEL API — STAY AHEAD OF EMERGING THREATS

The Falcon Intelligence API allows customers to benefit from a rich feed of information spanning indicators, adversaries, news and customizable threat intelligence. Visualization tool integration enables you to see correlations between adversaries, indicators, malware families and campaigns.

RESOURCES:

For more information visit

https://www.crowdstrike.com/products/falcon-connect/

INCREASE YOUR EXISTING SECURITY AND IT FUNCTIONALITY WITH FALCON PLATFORM APIS.

THIS SET OF POWERFUL AND EASY-TO-USE APIS ENABLES APPLICATIONS TO CONNECT WITH THE CROWDSTRIKE FALCON PLATFORM. FALCON APIS ENABLE CUSTOMERS TO TAKE FULL ADVANTAGE OF THEIR EXISTING SECURITY TOOLS AND DEVELOP AUTOMATION WORKFLOWS.