

Falcon Adversary Intelligence APIs

Integrate CrowdStrike's industry-leading threat intelligence seamlessly to enhance detection, response and proactive defense

Security teams are in a never-ending race against time to find and shut down threats. Today's adversaries are faster and stealthier than ever, using legitimate tools to carry out lightning-fast, hands-on-keyboard attacks, while staying under the radar, hiding from defenders.

Security teams burdened with legacy tools struggle to match the speed of attackers. As technology evolves, so do adversaries. The modern SOC is not just about operationalizing new technology — it's about defending against mutating malware, AI-driven phishing and data poisoning. Staying ahead means adapting swiftly to an ever-changing threat landscape.

CrowdStrike, a leader in threat intelligence, has over a decade of expertise in battling the most sophisticated nation-state and eCrime adversaries, protecting millions of endpoints, cloud workloads and identities. Threat intelligence is the foundation of the AI-powered CrowdStrike Falcon® platform, which delivers highly accurate detections, automated tooling and enriched threat context. The cloud-native CrowdStrike Falcon® Adversary Intelligence APIs enable security teams to detect and respond faster and more confidently, helping achieve the outcome that matters most: stopping breaches.

Timely, Relevant, Trusted Intelligence

CrowdStrike threat intelligence is derived from an elite group of collection experts, technologists, intelligence analysts and threat hunters. The team tracks 245+ named adversaries, thousands of malware families and hundreds of campaigns on a daily basis.

The team benefits from an unparalleled raw collection of intelligence data, regularly leveraging trillions of events per day from across 29,000+ global Falcon platform customers as well as real-world threat hunting and incident response insights.

Key benefits

- Industry-leading threat intelligence
- Enhanced detection and response
- Proactive defensive countermeasures
- Efficient malware analysis
- Scalable, flexible integrations

CrowdStrike's all-source intelligence collection is based upon:

- Telemetry from millions of endpoints around the globe, providing trillions of unique events weekly
- Tens of millions of malware samples per day analyzed by advanced sandbox technology
- Hundreds of incident response engagements annually
- Deep, dark web, covering criminal marketplaces, dedicated leak sites, paste sites, code repositories, forums and message boards
- A globally deployed sensor grid with extensive honeypot detection capabilities
- A constant flow of open-source intelligence (OSINT)

CrowdStrike's deep adversary knowledge, expertise in pursuing and stopping threats, and visibility derived from an all-source collection strategy make the company uniquely qualified to deliver the most effective countermeasures to stop breaches and protect customers.

Key APIs and Capabilities

Falcon Adversary Indicator API

The Indicator API provides access to CrowdStrike's near real-time indicator of compromise (IOC) feed, including the IOCs that drive detections within the CrowdStrike Falcon platform.

This RESTful API enables seamless integration into security controls such as SIEMs, network gateways, email security solutions and more. The IOCs are generated using a massively scaled malware analysis platform, and false positives are greatly reduced by ensuring the inputs are sourced only from within CrowdStrike and vetted by human analysis and machine learning. To further reduce false positives, CrowdStrike validates the generated IOCs against the telemetry of millions of endpoints protected globally by the Falcon platform.

The Indicator API enables developers to query various types of IOCs with robust filtering and sorting options, ensuring the delivery of the most relevant IOCs within the target environment.

Key Features

IOC Types	Total Indicators ¹	Description
File Hash	241 million	Known malicious MD5, SHA1 and SHA256 file hashes
URL	7.2 million	URL associated with malware or malicious activity
Domain	2.8 million	Malicious domain names
IP Address	885K	Malicious IP addresses
Mutex	111K	Malicious mutex names
Password	28K	Known passwords used by malware or adversaries
Additional IOC types include: File Name, Email Address, Username, Bitcoin Address, Coin Address, IP Address Block, Persona Name		
Metadata	Indicator type, published date, last updated date, related adversaries, malware family, kill chain techniques, confidence score, analyst applied threat labels, target industries, threat type, associated vulnerabilities, related IOCs	
Available Filters	Indicator type, actor, confidence score, published and last updated date, malware families, kill chain techniques, threat labels, threat type, targeted industries	

¹The value of IOCs is best measured by their quality, timeliness and uniqueness rather than their quantity. The provided quantity serves only as a reference for evaluating IOC feeds and is valid as of July 15, 2024.

"CrowdStrike has more than 10 years in the Cyber Threat Intelligence industry and it continues to dominate in this space. Its threat intelligence is actionable, automated, and built into daily workflows, powering the company's broad cybersecurity portfolio."

– Frost & Sullivan naming CrowdStrike the 2022 Global Company of the Year in Cyber Threat Intelligence

Benefits:

- CrowdStrike-validated IOCs
- Unique indicators — CrowdStrike does not use third-party or open source feeds
- Built-in adversary attribution
- IOC enrichment delivering context for threat hunting and effective IR response
- No API consumption limits

Use Cases: Prevention, Detection, Threat Hunting

Falcon Adversary Actor API

The Actor API offers access to hundreds of detailed actor profiles, containing the latest insights into the tactics, techniques and procedures used by today's most sophisticated adversaries. These profiles equip security teams with the essential context and information needed to proactively defend against, investigate and respond to continuously evolving threats.

This API enables organizations to proactively identify potential adversaries and prioritize system hardening based on known attack vectors, and it enables users to pivot from the CrowdStrike indicator feed to deliver valuable context about adversaries' motivation and tradecraft.

Key Features

Adversary Profiles	245+ profiles across nation-state actors, eCrime groups and hacktivists
Metadata	Adversary name, alternative names, description, capability, created date, activity status, kill chain techniques, target industries, actor group, region, origins, target countries, motivations, first and last activity date, last modified

Benefits:

- Profiles are continuously updated with the latest tradecraft
- Details the tactics, techniques and procedures
- Delivers required context to enable a proactive defense and incident response
- Helps identify which systems and data are most likely to be targeted

Applicable Use Cases: Proactive Threat Hunting, Incident Response and Investigation, Strategic Defense Planning

Falcon Adversary Vulnerability Intelligence API

The Vulnerability Intelligence API provides the latest exploitation details with real-time updates sourced from the National Vulnerability Database. CrowdStrike's exploit insights are continually updated based upon expert assessments and real-time telemetry. The API provides an exploit status, affected products and vendors, when a vulnerability was published and any related threats or adversaries.

This API enables users to prioritize existing attack surface vulnerabilities more effectively and prepare for highly productive patching cycles.

Key Features

CVEs Published	Over 250,000
Metadata	CVE, exploit status, related threats, related actors, published date, updated timestamp, affected products (vendor, product), severity, CVSS score, description

Benefits:

- Proactively patch or mitigate systems
- Understand the severity, potential impact and exploitability
- Enhance incident response

Applicable Use Cases: Patch Management and Prioritization, Threat Assessment, Incident Response, Forensics

Falcon Adversary Intelligence Sandbox API

The Sandbox API performs deep analysis of evasive and unknown threats. Files are detonated in a safe and secure environment hosted by CrowdStrike. All files and reports remain private. The output of the analysis includes the verdict, generated IOCs and a comprehensive analysis report. These reports include incident response summaries, adversary attribution, detonation screenshots, network traffic analysis, extracted stings and memory dumps, and much more.

Unique to the sandbox is its ability to analyze, identify and find related files. For every file submitted for analysis, the Sandbox API will query CrowdStrike's data store of 8.5 billion malware samples to find files within the same malware family, author, polymorphic samples or updated versions, even malware that shares similar code or infrastructure. This enables users to expand their protection by generating a more comprehensive set of IOCs.

Key Features

Detecting Unknown Threats	▪ Hybrid-Analysis: Combines runtime data, static analysis and memory dump analysis to extract all possible execution pathways ▪ Anti-Evasion Technology: Provides file monitoring that runs in the kernel and cannot be observed — CrowdStrike continuously tests each release to ensure the sandbox is nearly undetectable by malware ▪ User Interactivity: Enables control of how malware gets detonated to avoid malware hiding from sandboxes
Reporting	▪ Prioritization: Delivers verdict and threat scores ▪ Comprehensive Reporting: Provides identified intrusion techniques, extracted files, screenshots, memory captures and stack traces ▪ IOCs: Generates IOCs from submitted malware, available in industry standard formats ▪ MITRE Mapping: Maps behavior to MITRE ATT&CK tactics and techniques ▪ Related Malware: Searches across CrowdStrike's database of 8.5 billion malware samples to identify similar malware
Data Privacy and Retention	All submitted files and associated reports are stored and maintained in this separate environment and are completely private and secure.

Supported Operating Systems: Windows

File Types: Executables (exe, .scr, .pif, .dll, .com, .cpl, etc.), Office (.doc, .docx, .ppt, .pps, .pptx, .ppsx, .xls, .xlsx, .rtf, .pub), PDF, APK, executable JAR, Windows Script Component (.sct), Windows Shortcut (.lnk), Windows Help (.chm), HTML Application (.hta), Windows Script File (*.wsf), Javascript (.js), Visual Basic (*.vbs, *.vbe), Shockwave Flash (.swf), Perl (.pl), PowerShell (.ps1, .psd1, .psm1), Scalable Vector Graphics (.svg), Python (.py) and Perl (.pl) scripts, Linux ELF executables, MIME RFC 822 (*.eml) and Outlook *.msg files

Archives Supported: ace, arj, 7z, bzip2, gzip2, iso, rar, rev, tar, wim, xz and zip

Output formats: CSV, JSON, MAEC 5.0, STIX 2.1, PCAP

Benefits:

- Provides a safe and isolated detonation environment
- Exposes malware behavior to understand tactics and impact, leading to more effective defense
- Enables quick identification and classification of malware

Applicable Cases: Malware Analysis and Research, Incident Response and Forensics, Automated Threat Detection

Falcon Adversary Intelligence QuickScan ML API

There is a growing need for organizations to evaluate potentially malicious files and render a verdict (clean, potentially unwanted, malware) in near real time — especially when performing a full sandbox analysis is overkill. The QuickScan ML API can either work standalone to evaluate potentially malicious files or work in concert with the Sandbox API by forwarding potentially unwanted files to the sandbox for full analysis.

Key Features

Near Real-Time Analysis	The QuickScan ML API is used when speed is critical. It typically takes QuickScan ML milliseconds to render a file verdict, enabling file analysis at scale. Use cases: - Provides file validation upon upload/download from a website - Quickly verifies whether an email attachment is malicious before delivery, scans the contents of a folder or directory at scale
Analysis Orchestration	Optimize the malware analysis pipeline for speed and efficiency: Triage with QuickScan ML: Triage the potentially malicious file with the QuickScan ML API. Submit for Full Analysis: Any files flagged as potential threats during the triage process can be submitted to the Sandbox API for comprehensive analysis. This ensures a thorough examination and response to any identified malware. This optimized flow enhances the speed and efficiency of the malware analysis process, ensuring swift detection and response to threats.

Benefits:

- High level of accuracy
- Early detection of malicious code
- Safe and non-intrusive
- Highly scalable

Operating Systems Supported: Windows, Mac and Linux

File Types Supported: Windows (PE and dll), Mac (*Mach-O), Linux (elf) document files (.pdf, .doc, .docx, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm) and image files (.bmp, .gif, .jpeg, png, .tiff)

Applicable Use Cases: File validation upon upload/download; file analysis on email attachments, directory or bulk scanning; file analysis flow optimization

LEARN MORE →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.