CROWDSTRIKE

CROWDSTRIKE FALCON INTELLIGENCE

CrowdStrike Falcon Intelligence integrates threat intelligence into endpoint protection, automating incident investigations and speeding breach response

CROWDSTRIKE FALCON INTELLIGENCE

MAKING PREDICTIVE SECURITY A REALITY

For cyber protection teams that are struggling to respond to cybersecurity alerts and don't have the time or expertise to get ahead of emerging threats, the CrowdStrike Falcon Intelligence™ solution delivers the critical intelligence you need, while eliminating the resource-draining complexity of incident investigations. Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response, and enabling security teams to move from a reactive to a predictive, proactive state.

With the unique cloud-native CrowdStrike Falcon® platform as a foundation, cyber protection teams can now automatically analyze malware found on endpoints, find related samples from the industry's largest malware search engine, and enrich the results with customized threat intelligence. This closed-loop system provides security teams with custom indicators of compromise (IOCs) to share with their other security tools as well as intelligence reporting that tells the complete story of the attack. With a complete understanding of the attack, your team is empowered to respond faster and orchestrate proactive countermeasures across your organization.

Falcon Intelligence and integrated threat intelligence is the next step for endpoint protection. It takes antivirus and endpoint detection and response alerts to the next level by not only showing what happened on the endpoint, but also revealing the "who, why and how" behind the attack. Understanding the threat at this level is the key to getting ahead of future attacks and raising the cost to the adversary.

Falcon Intelligence enables customers of all sizes to better understand the threats they face and improves the efficacy of their other security investments with actionable and customized intelligence to defend against future attacks, making proactive security a reality.

KEY BENEFITS

- Automates investigations into all threats that reach your endpoints
- Delivers custom IOCs to proactively guard against evasive threats
- Provides complete information on attacks to enable faster, better decisions
- Empowers your team with analysis from CrowdStrike® Intelligence experts
- Simplifies operations via seamless integration with the CrowdStrike Falcon platform

KEY PRODUCT CAPABILITIES

AUTOMATE AND SIMPLIFY INCIDENT INVESTIGATIONS

Seamless endpoint Integration:
Analyze high-impact threats taken directly from your endpoints that are protected by the CrowdStrike Falcon platform. Falcon Intelligence analysis is presented as part of the detection details of a Falcon endpoint protection alert. Security teams, regardless of size or skill level, will never miss an opportunity to learn from an attack in their environments.

Save time, effort and money:
Automate each step of a cyber threat investigation and reduce analysis time from days to minutes. Falcon Intelligence combines malware analysis, malware search and threat intelligence into a seamless solution.

Stop bad actors in their tracks:
CrowdStrike threat intelligence provides actor attribution to expose the motives, tools and tradecraft of the attacker. Practical guidance and proactive steps are prescribed so your team can deploy proactive countermeasures and get ahead of future attacks.

SHARE CUSTOM IOCs FOR SECURITY ORCHESTRATION

Defend against the most relevant threats
Focus your team on threats you actually encountered. Falcon Intelligence delivers custom IOCs that are derived from the automated analysis of threats taken directly from your endpoints. Custom IOCs include protection against the threat you just encountered plus related threats within the same campaign or malware family. This exclusive capability leads to a deeper understanding of the threat and a custom set of IOCs to defend against future attacks.

Gain access to CrowdStrike IOCs
Falcon Intelligence allows you to expand your defenses with real-time access to global IOCs delivered by CrowdStrike.

Easily integrate countermeasures
Protect against future attacks with IOCs that are easily consumed by your security infrastructure. A rich suite of APIs and pre-built tools enable easy orchestration with existing security solutions.

EMPOWER YOUR TEAM WITH CROWDSTRIKE THREAT INTELLIGENCE

Intelligence Reports	Receive trusted, in-depth threat intelligence reports from the global CrowdStrike Intelligence team, including real-time threat alerts, technical reports with expert analysis, and strategic reports outlining threats to industries, regions and infrastructure.
Threat Monitoring	Monitor the web for adversary activity against your organization to prioritize resources and effectively respond to impending cyberattacks.
Expert Malware Analysis	Escalate interesting malware samples to a CrowdStrike expert for deeper research or to get a second opinion.
Intelligence Support	The CrowdStrike team works to ensure it has a clear understanding of your intelligence requirements and that you are successfully onboarded. The team also performs quarterly reviews.
YARA/SNORT Rules	Keep ahead of the latest adversary threats and orchestrate your defenses with YARA and SNORT rules, created and validated by CrowdStrike experts.

Start Free Trial
of Falcon Intelligence

Learn more at **www.crowdstrike.com**

FALCON INTELLIGENCE — PRODUCT OFFERINGS

There are two levels of Falcon Intelligence, enabling your organization to choose the option that best fits your needs and mission requirements.

Feature	Falcon Intelligence	Falcon Intelligence Premium
Endpoint Integration	X	X
Intelligence Automation	X	X
Custom Intelligence	X	X
Custom and Global IOCs	X	X
Intelligence Reports		X
Threat Monitoring		X
Intelligence Support		X
Expert Malware Analysis		X
YARA/SNORT Rules		X
Quarterly Briefings		X

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/