CROWDSTRIKE

CrowdStrike Products

Data Sheet

Falcon Adversary Intelligence

Reduce detection, investigation, and response time with personalized threat intelligence and AI-powered workflows

Challenges

Today's adversaries move with speed and sophistication, exploiting weak points faster than most security teams can respond. In 2024, the average eCrime breakout time dropped to just 48 minutes, and 79% of attacks used no malware.[1] As attackers grow stealthier, defenders are slowed by manual processes, siloed tools, and intelligence that lacks relevance.

Smaller teams often rely solely on their security tools, while larger organizations may invest in legacy SIEMs to detect and investigate attacks. Yet over 60% of these systems generate more than 1,000 alerts daily,[2] overwhelming SOC teams and delaying response.

To make matters worse, 80% of organizations limit their intelligence to known threats, missing signals of evolving adversary behavior.[3] Disrupting modern attacks requires real-time insight into adversary tradecraft — and the ability to apply that intelligence within your specific environment.

Threat intelligence is no longer optional. It's essential for closing gaps, accelerating response, and staying ahead of active threats.

Key benefits

- **Accelerate triage and investigation** with personalized intelligence that reduces noise and highlights what matters most
- **Prioritize threats based on relevance,** enabling faster decisions and more effective response actions
- **Safeguard your brand** with continuous monitoring of the dark web and criminal ecosystems to uncover external threats targeting your organization
- **Deploy precise defenses** with pre-built workflows that align intelligence to your tools, teams, and environment

[1] CrowdStrike 2025 Global Threat Report

[2] Gurucul, 2023 SIEM Data Analytics Challenges Facing the SOC

[3] ESG Research, Operationalizing Cyber-Threat Intelligence, March 21, 2023

Solution

CrowdStrike Falcon® Adversary Intelligence delivers personalized, real-time threat intelligence aligned to your unique environment and risk profile. Whether used within the CrowdStrike Falcon® platform or integrated into third-party tools, it accelerates detection, investigation, and response with high-fidelity, actionable intelligence.

While all organizations benefit from CrowdStrike's industry-leading intelligence, its impact grows when added to the AI-native Falcon platform — making other Falcon modules intelligence-aware from Day One. Analysts receive prioritized intelligence tailored to their role and mission, enabling faster, more confident decisions.

By integrating intelligence into daily workflows, Falcon Adversary Intelligence reduces manual effort and sharpens focus. Customers have achieved up to a 97% reduction in adversary research time, up to an 80% decrease in malware analysis time, and up to 79% reduction in triage effort.[4]

Whether augmenting a SIEM, streamlining SOC workflows, or enhancing threat hunting, Falcon Adversary Intelligence adapts to your environment — not the other way around.

Key capabilities

Expose the Threats that Matter Most

Falcon Adversary Intelligence reduces risk by delivering actionable insight into your attack surface, the adversaries targeting it, and the threats most relevant to your organization. Defend proactively with targeted intelligence and recommendations tailored to your environment.

- **Personalized threat modeling:** Automatically surface adversary risk signals specific to your business. CrowdStrike's automated threat modeling helps you cut through the noise, prioritize what matters, and take informed action with tailored guidance.
- **Attack surface reduction:** Strengthen your defenses with intelligence that includes adversary profiles, credential monitoring, vulnerability insights, and context-rich indicators aligned to your environment.
- **Unified intelligence workspace:** Accelerate investigation with CrowdStrike Intelligence Explorer, a centralized interface for exploring indicators, adversaries, malware, and related vulnerabilities — enabling faster triage and smarter decisions through dynamic pivoting.
- **Context-rich indicator of compromise (IOC) investigations:** Investigate indicators with full context — including related adversaries, kill chain overlays, and observed activity — via the Indicator app, enabling deeper insights and faster response.

[4] These numbers reflect the median inputs provided by customers during pre- and post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

Streamline Your SOC Through Automation

With end-to-end automation, Falcon Adversary Intelligence cuts response time from days to minutes across your entire security stack. Instantly submit potential threats to an advanced sandbox, extract indicators, and deploy countermeasures automatically across your security stack.

- **Advanced malware sandbox:** Seamlessly integrated into your security operations, the sandbox automates file, email, and command-line analyses within seconds, enables quick triage, and provides essential context for informed next steps.
- **Indicator API:** This API provides seamless access to CrowdStrike's real-time IOC feed, powered by advanced malware analysis, global telemetry, and rigorous human and machine validation, ensuring accurate and actionable threat intelligence for integration into security controls.

Protect Your Brand, Employees, and Sensitive Data

Falcon Adversary Intelligence's Recon feature delivers continuous monitoring across the open, deep, and dark web, enabling security teams to proactively identify and respond to external threats. From fraud and phishing campaigns to data leaks and brand impersonation, Recon helps you stay ahead of adversaries targeting your organization.

- **Brand and fraud monitoring:** Gain real-time visibility beyond your perimeter to uncover domain impersonation, exposed credentials, and sensitive data leaks — before they can be exploited.
- **Automated takedowns and blocklist submissions:** Proactively reduce threat exposure by reporting malicious domains and submitting blocklists. CrowdStrike initiates automated takedowns through registrars, hosting providers, and SSL issuers to remove malicious content such as phishing sites and fake profiles. Blocklist submissions also engage third-party providers — including email platforms, browsers, registrars, and industry groups — to quickly restrict access to harmful domains.
- **Risk-based monitoring:** Recon automatically aligns to your organization's unique risk profile, eliminating manual setup and helping teams focus immediately on the most relevant external threats.

Seamlessly Integrate with Third-Party Tools

Accelerate response and reduce complexity with prebuilt playbooks, open APIs, and streamlined workflows that work across your existing security stack — whether or not you're using the CrowdStrike Falcon platform.

- **Prebuilt playbooks:** Improve consistency and scale response with ready-to-use incident response playbooks that simplify orchestration and automate countermeasures — without the need for custom integrations.
- **Flexible API integration:** Push relevant IOCs and intelligence to the right tools at the right time. Whether you're using CrowdStrike Falcon® Fusion SOAR, a third-party SOAR, or other tools, CrowdStrike helps automate defense actions across your SOC.

CrowdStrike Threat Intelligence Products and Services

Feature Categories	Key Features	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Counter Adversary Operations Elite[5]
Threat Intelligence	In-Depth Adversary Profiles	✓	✓	
	Weekly Threat Summaries	✓	✓	
	Threat Landscape Dashboards	✓	✓	
	Intelligence Reports		✓	
	Quarterly Threat Briefs		✓	
	Threat Hunting Libraries		✓	
	Requests for Information (5 Pack)		Ability to add	✓
	Priority Intelligence Requirements			✓
	Threat Graph Queries (Up to 50)			✓
Digital Risk Protection	Dark Web Monitoring	✓	✓	
	Brand and Domain Monitoring	✓	✓	
	Credential Monitoring	✓	✓	
	Dark Web Activity Reports	✓	✓	
Automation and Tools	Malware Sandbox	✓	✓	
	Indicator of Compromise App	✓	✓	
	Vulnerability Intelligence App	✓	✓	
	QuickScan Pro Analysis	1,000/month	2,500/month	
	Threat Feed (IOCs)	✓	✓	
	APIs and Integrations	✓	✓	
	Human Malware Analysis (50 per Year)		✓	
	Pre-Built Detection Rules (YARA, Snort)		✓	
Assigned Analyst	Access Analyst via Email			✓
	Customer-Directed Threat Hunts			✓
	Threat Hunt Query Optimization			✓
	External Digital Risk Investigations			✓
	Tailored Threat Briefings and Risk Reports			✓

[5] Falcon Adversary Intelligence Premium is a prerequisite for Falcon Counter Adversary Operations Elite.

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.

CrowdStrike: We stop breaches.

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

Follow us: Blog | X | LinkedIn | Facebook | Instagram

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