CROWDSTRIKE

CrowdStrike Products

Data Sheet

Falcon Adversary Intelligence

Optimize the effectiveness of your security operations center through the power of threat intelligence and AI automation

Challenges

Adversaries have become faster and more sophisticated, consistently outpacing organizations and breaching their defenses. As endpoint surfaces harden with advanced security like endpoint detection and response (EDR) and Zero Trust, adversaries exploit new ways to break in and evade detection, further complicating defense efforts. Being slower than the adversaries poses significant risks to your brand, reputation and financial standing.

Smaller organizations rely solely on their security tools for protection, while larger entities invest heavily in traditional security information and event management (SIEM) tools to detect and investigate attacks. Unfortunately, these legacy SIEMs aren't up to the task. An estimated 61% of legacy SIEMs generate more than 1,000 alerts daily,[1] overwhelming understaffed and underskilled SOC teams, and resulting in slower operations and missed threats.

Additionally, 80% of organizations limit their understanding of threat intelligence to known threats.[2] But intelligence must go beyond the basics to provide real-time insight into adversaries' methods, and it must be applied in organizations' environments and SIEMs. Automation is key for shortening the time from detection to response, enabling the immediate deployment of countermeasures.

Solution

CrowdStrike Falcon® Adversary Intelligence optimizes the effectiveness of your security operations center through automated intelligence orchestration, contextual enrichment and advanced AI-powered investigative tools.

Every organization can benefit from the industry-leading threat intelligence provided by Falcon Adversary Intelligence — and when combined with the AI-native CrowdStrike Falcon® platform, the impact is significantly amplified. Falcon Adversary Intelligence delivers industry-leading threat intelligence into the Falcon platform, making all modules intelligence-aware on Day One. This integration empowers SOC teams with actionable context for confident, data-driven decisions, seamlessly embedded into daily operations.

With Falcon Adversary Intelligence, organizations are empowered to maximize their SIEM investments. CrowdStrike customers have experienced up to a 97% reduction in research time on adversaries and threats, up to 80% decrease in malware analysis time and up to 79% reduction in threat triage effort.[3]

Key benefits

- Falcon Adversary Intelligence cuts response time from days to minutes across your entire security stack through end-to-end intelligence automation.
- Digital risk protection capabilities proactively safeguard your brand, assets and reputation through automated monitoring of malicious activity across the dark web to uncover external threats targeting your organization.
- Pre-configured workflows deploy precise defenses at the right time and place, ensuring timely protection against emerging threats.

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

[2] ESG Research, Operationalizing Cyber-threat Intelligence

[3] Based on CrowdStrike Business Value Assessments (BVAs). CrowdStrike BVA numbers are projected estimates of average benefits based on aggregated business value assessments completed with customers 6+ months post deployment where they report realized process efficiencies compared to the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

Key capabilities

Streamline Your SOC Through Automation

Falcon Adversary Intelligence cuts response time from days to minutes across your entire security stack with end-to-end automation. Instantly submit potential threats to an advanced sandbox, extract indicators and deploy countermeasures — all while continuously monitoring for fraud and protecting your brand, employees and sensitive data.

- **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 indicator of compromise (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.

Get Digital Risk Protection

The Falcon Adversary Intelligence Recon feature delivers comprehensive digital risk protection (DRP) by exposing malicious activity across the open, deep and dark web. It empowers security teams to proactively detect and mitigate threats to their brand, employees and sensitive data. With Recon, you can stay ahead of adversaries by detecting fraud, data breaches, phishing campaigns and other online threats targeting your organization.

- **Brand and fraud monitoring:** Get enhanced threat visibility beyond your perimeter with real-time intelligence to uncover domain impersonations, exposed credentials and data leakages.
- **Automated takedowns and blocklist submissions:** Proactively reduce exposure to threats by reporting malicious domains and submitting blocklists. CrowdStrike will trigger automated takedowns with registrars, hosting providers and SSL certificate issuers, removing malicious content such as phishing sites and fake profiles. Blocklist submissions enable CrowdStrike to engage third-party providers — including email services, web browsers, registrars and industry working groups — to rapidly restrict access to harmful domains.
- **Covert, real-time investigations:** Access raw intelligence in real time to disrupt adversaries before they act. Gain covert, undetectable access to restricted sites and preserve historical data, ensuring adversaries can’t erase their tracks by altering or deleting posts.

Integrate Seamlessly with Third-Party Tools

Access a prebuilt library of incident response playbooks, empowering teams to orchestrate actions and automate defenses. Streamline responses with preconfigured workflows, eliminating the need for complex integrations.

- **Out-of-the-box playbooks:** Scale response quality with standardized playbooks, and consistently deploy countermeasures to optimize protection.
- **Security operations APIs:** Accelerate threat response by pushing the right IOCs to the right tools at the right time. Seamlessly automate defenses across your security operations center with CrowdStrike Falcon® Fusion SOAR playbooks and prebuilt integrations.

Proactively Reduce Risk with Comprehensive Intelligence

Falcon Adversary Intelligence reduces risk by delivering actionable insights into your attack surface, adversary infrastructure and threat prioritization. Proactively defend your organization with targeted threat intelligence and tailored recommendations.

- **Attack surface reduction:** Get threat intelligence capabilities that include adversary profiles, credential monitoring, context-aware indicators and vulnerability intelligence.
- **Exposure of adversary infrastructure:** Utilize attack surface scans to explore and identify adversary-controlled domains and high-risk infrastructure accessed by your organization.
- **Automated threat modeling:** Effortlessly surface adversarial risk from the noise with CrowdStrike's automated threat modeling. Rapidly identify the most critical threats specific to your business and get tailored recommendations.

CrowdStrike Threat Intelligence and Hunting: Products and Services

Feature Categories	Key Features	Falcon Adversary OverWatch	Falcon Adversary OverWatch Identity[1]	Falcon Adversary OverWatch Cloud	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Counter Adversary Operations Elite[2]
Threat Hunting	24/7 Managed Threat Hunting	✓	✓	✓			
	- Falcon Insight XDR	✓					
	- Falcon Identity Protection		✓				
	- Falcon Cloud Security			✓			
Threat Intelligence	Adversary Cards	✓					
	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	Analyst Access via Email, SMS and Phone						✓
	Customer-Directed Threat Hunts						✓
	Threat Hunt Query Optimization						✓
	External Digital Risk Investigations						✓
	Tailored Threat Briefings and Risk Reports						✓

[1] Falcon Adversary OverWatch or Falcon Adversary OverWatch Cloud is a prerequisite for Falcon Adversary OverWatch Identity.
[2] 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/