

Falcon Counter Adversary Operations Elite

Disrupt sophisticated adversaries with a powerful ally on your side

Challenges

Today's adversaries are increasingly fast and elusive, continuously adapting their motives and tactics. Their evolving techniques represent a significant challenge in the modern threat landscape.

According to the [CrowdStrike 2025 Global Threat Report](#), 52% of vulnerabilities exploited in 2024 were tied to initial access, with valid account abuse driving 35% of cloud intrusions. Once inside, adversaries moved fast — the fastest observed eCrime breakout time was just 51 seconds. New and unattributed cloud intrusions rose 26% year-over-year, driven by misconfigurations, stolen credentials, and abuse of cloud management tools.

As adversaries demonstrate greater proficiency and speed in targeting organizations, it is imperative that defenders stay one step ahead to proactively stop breaches.

Solution

A truly effective cybersecurity program requires relevant, timely, and actionable threat intelligence, but tracking scores of adversaries and analyzing their tradecraft requires a massive effort. CrowdStrike Falcon® Counter Adversary Operations Elite was created to help you focus on what matters most — threats targeting your organization.

Key benefits

- Falcon Counter Adversary Operations Elite pairs you with an assigned analyst armed with deep adversary intelligence and industry-leading threat hunting capabilities to disrupt adversaries targeting your business
- Your assigned analyst acts as an extension of your team, accelerating investigations, enabling rapid attribution, and delivering personalized intelligence to keep you steps ahead of the adversary
- By conducting real-time, tailored threat hunts powered by CrowdStrike's intelligence, your analyst proactively uncovers sophisticated intrusions — before they cause harm
- Your analyst extends protection beyond your network with deep visibility into criminal forums and the dark web to hunt emerging threats targeting your business

The CrowdStrike team is staffed by seasoned analysts with unsurpassed expertise battling nation-state, eCrime, and hacktivist adversaries. An Elite analyst works directly with your team to learn the unique cybersecurity challenges your organization faces. This understanding enables the analyst to help you apply threat intelligence more effectively, defeating the adversaries targeting your organization.

The Elite analyst is your point of contact for intelligence research, threat hunting, detection engineering, and personalized threat briefings. The analyst also provides proactive notifications of threats against your organization — going beyond consultation to become an extension of your team.

Key product capabilities

Trusted Strategic Advisor

- **Assigned CrowdStrike Elite analyst:** Your organization gains access to an assigned analyst that delivers relevant, timely, and actionable intelligence. This analyst leverages an in-depth understanding of your security needs and performs tailored research on your behalf.
- **Personalized security insights:** Leveraging threat intelligence tailored to your organization, the analyst pinpoints potential adversary tactics and risks specific to your industry, region, and exposure. A continuous feedback loop with threat hunting queries further enriches this process, enhancing your defense against sophisticated attacks.

Intelligence-Driven Defense

- **Requests for information (RFIs):** Threat intelligence research can be difficult, and CrowdStrike can provide assistance. An RFI is a request for CrowdStrike to perform research, on your behalf, into a specific threat to your organization. You can have up to 5 RFIs per year, and additional packs are available for purchase. The research is performed by a domain expert who delivers a custom response.
- **Priority intelligence requirements (PIRs):** PIRs align the activities of threat intelligence teams to the goals and strategies of your organization. Your Elite analyst helps you create PIRs — or leverage knowledge of existing PIRs — to provide proactive notifications of threat activities that may target your organization, employees, or infrastructure. Examples of PIRs include:
 - Which nation-state threat actors are targeting your region or industry?
 - Are there threats to your organization from criminal underground sites monitored by CrowdStrike?
 - Which tactics and techniques are adversaries likely to use to exploit your infrastructure?
- **Threat briefings:** One-on-one threat briefings expose the latest adversarial activities relevant to your industry and region, delivering rich context, clearer visibility into related risks, and recommendations aligned to your environment. Leveraging these insights, you can enhance your defenses against targeted threats and inform leadership of the critical risks to your business.

Managed Threat Hunting

- **Proactive and tailored threat hunting:** Facing ever-evolving adversaries, your assigned analyst detects new and sophisticated intrusions in real time, using hunting guides and custom hunts specifically designed for your environment.

CrowdStrike Products

Falcon Counter Adversary Operations Elite

- **CrowdStrike Threat Graph® inquiry:** The AI-powered CrowdStrike Falcon® platform regularly analyzes trillions of security events from across the globe every day. The Elite analyst searches this data to determine the prevalence of a specific indicator of compromise (IOC) globally or within your sector or region.

Hunt Beyond the Perimeter

- **Digital risk protection:** Elite analysts monitor data from thousands of external sources, including restricted criminal forums and social media, to give you real-time warnings about potential threats to your brand, employees, and sensitive data.
- **Takedown facilitation:** CrowdStrike works on your behalf to identify and facilitate the takedown of fraudulent accounts, phishing websites, domains, and malicious posts that can harm your reputation or business.

CrowdStrike Threat Intelligence Products and Services

Feature Categories	Key Features	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Counter Adversary Operations Elite ¹
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			✓

¹ Falcon Adversary Intelligence Premium is a prerequisite for Falcon Counter Adversary Operations Elite.

Attend a hands-on workshop →

Request a demo of other Counter Adversary Operations offerings →

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/>

