CROWDSTRIKE

CrowdStrike Products
Data Sheet

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.

Adversaries' breakout time continues to get faster. According to the CrowdStrike 2024 Global Threat Report, the fastest observed time for an adversary to start moving laterally was just over 2 minutes in 2023, and in 75% of attacks, threat actors gained initial access using malware-free techniques. As organizations strengthen their environments, adversaries explore new attack vectors — CrowdStrike observed a 75% year-over-year increase in cloud intrusions in 2023 and also saw an uptick in attacks using compromised identities and unmanaged systems.

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 (CAO) Elite was created to help you focus on what matters most — threats targeting your organization.

Key benefits

- Falcon Counter Adversary Operations Elite provides **access to an assigned analyst** with deep adversarial intelligence and advanced threat hunting tools to disrupt adversaries targeting your business
- Your assigned analyst enables you to **respond faster with rapid investigation and attribution**, leveraging extensive adversary intelligence to keep you steps ahead
- **Your analyst detects new and sophisticated intrusions in real time**, using custom hunts developed from industry-leading threat intelligence
- **Extending protection beyond your network perimeter**, your analyst hunts for threats using unprecedented visibility into criminal forums

The Falcon CAO Elite team is staffed by seasoned analysts with unsurpassed expertise battling nation-state, eCrime and hacktivist adversaries. A Falcon CAO 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 Falcon CAO 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 CAO 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.
- **Tailored security insights:** Filtering through extensive intelligence, the analyst pinpoints potential adversary tactics and risks specific to your geographic location and sector. 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 Falcon CAO 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 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 and the threats targeting your industry and region. Leveraging these insights, you can enhance your defenses against targeted threats and inform leadership of the relevant 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 custom hunts specifically designed for your environment.

- **CrowdStrike Threat Graph® inquiry:** CrowdStrike's AI-powered Falcon platform regularly analyzes trillions of security events from across the globe every day. The 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:** Falcon CAO 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.

Attend a hands-on workshop

Request a demo of other CAO 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/