

CrowdStrike Brings Together Cybersecurity's Market Leading Threat Intelligence, Threat Hunters and AI to Unleash New CrowdStrike Counter Adversary Operations

August 8, 2023

The market leader in threat intelligence and pioneer in managed threat hunting debuts first-of-its kind team and offerings to stop modern breaches and raise adversaries' cost of doing business

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Aug. 8, 2023-- BLACK HAT USA -- [CrowdStrike](#) (Nasdaq: CRWD), a market leader in threat intelligence and pioneer in managed threat hunting today announced another cybersecurity first, with the launch of CrowdStrike Counter Adversary Operations. The new team and offerings bring together CrowdStrike [Falcon@ Intelligence](#), the CrowdStrike [Falcon@ OverWatch](#) managed threat hunting teams and trillions of the latest telemetry events from the AI-powered CrowdStrike Falcon@ platform to detect, disrupt and stop today's sophisticated adversaries in their tracks and ultimately raise their cost of doing business.

The launch of the new Counter Adversary Operations comes fresh on the heels of CrowdStrike being named a leader in [The Forrester Wave: External Threat Intelligence Service Providers, Q3 2023](#). CrowdStrike received the highest ranking of all vendors in the Current Offering category, with the highest score possible in 16 criteria, surpassing all other vendors evaluated in the report.

"From our inception, CrowdStrike's guiding philosophy has been, 'You don't have a malware problem, you have an adversary problem,' and that has never been more true than it is today. Today's threat actors are increasingly fast and elusive, their motives are rapidly shifting from even 12 months ago, and the tradecraft we're seeing in the wild is far too often bypassing legacy and even modern security measures," said Adam Meyers, head of Counter Adversary Operations, CrowdStrike. "To beat modern adversaries at their game, threat intelligence needs to go past understanding the threat to rapidly actioning threat hunters to disrupt and stop the threat. The newly formed Counter Adversary Operations represents a new model that not only brings together the very best adversary insight and expertise on the planet – gleaned from deep threat intelligence, hands-on-keyboard activity and trillions of telemetry events – but one that rapidly puts this insight into that hands of teams on the front lines to protect against modern threats while making life increasingly hard on the adversary."

In the just released [CrowdStrike 2023 Threat Hunting Report](#), CrowdStrike revealed massive year-over-year increases in identity-based attacks, interactive intrusions (i.e. hands-on-keyboard activity) and increased use of legitimate remote monitoring and management (RMM) tools – all while breakout time dropped to a record low. Specifically, the report – the first under the new Counter Adversary Ops team – found a 583% year-over-year increase in Kerberoasting attacks, a technique adversaries can abuse to obtain valid credentials for Microsoft Active Directory service accounts. Overall, 62% of all interactive intrusions involved the abuse of valid accounts, while breakout time – the average time it takes an adversary to move laterally from initial compromise – fell to 79 minutes, and the fastest breakout observed was a stunning 7 minutes.

First new Counter Adversary Operations offering announced: Identity Threat Hunting

In response to the growing popularity of identity-based attacks and the increasing sophistication of adversary tradecraft CrowdStrike is seeing in the wild, CrowdStrike Counter Adversary Operations introduced its first new offering: Identity Threat Hunting. Immediately available as part of [CrowdStrike Falcon OverWatch Elite](#), the offering brings together the latest intelligence on adversary TTPs and motives, combined with CrowdStrike Falcon Identity Threat Protection and CrowdStrike's elite Falcon OverWatch threat hunters to thwart the latest identity-based threats.

The new offering makes it possible to quickly identify and remediate compromised credentials, track lateral movement, and outpace adversaries with always-on, 24/7 coverage. And, this service is available to new and existing CrowdStrike Falcon OverWatch Elite customers at no additional cost.

The new Identity Threat Hunting offering is the first of many accelerated innovations being introduced by Counter Adversary Operations that will quickly close the loop between what CrowdStrike researchers find in the wild and new customer-focused innovation within the Falcon platform.

Additional Resources

- Read a [blog](#) on CrowdStrike's Counter Adversary Operations, identity threat hunting offering and threat hunting report.
- Download your copy of the [2023 CrowdStrike Threat Hunting Report](#).
- Listen to the [Adversary Universe podcast](#). New episodes drop bi-weekly on Thursdays.
- Find out more about [CrowdStrike Falcon OverWatch Elite](#).
- Register [here](#) to join the CrowdStrike CAO team for a live CrowdCast on August 23 in North America or August 24 in EMEA and APJ for insights from the 2023 Threat Hunting Report.

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 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](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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

© 2023 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

View source version on [businesswire.com](https://www.businesswire.com/news/home/20230808148812/en/): <https://www.businesswire.com/news/home/20230808148812/en/>

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike