CROWDSTRIKE
Investor Relations

CrowdStrike and Microsoft Collaborate to Harmonize Cyber Threat Attribution

June 2, 2025

Landmark industry collaboration maps threat actor aliases across vendors to accelerate response and strengthen global cyberdefense

AUSTIN, Texas--(BUSINESS WIRE)--Jun. 2, 2025-- CrowdStrike (NASDAQ: CRWD) and Microsoft today announced a collaboration to bring clarity and coordination to how cyber threat actors are identified and tracked across security vendors. By mapping threat actor aliases and aligning adversary attribution across platforms, the collaboration minimizes confusion caused by different naming systems and accelerates cyber defenders' response against today's and tomorrow's most sophisticated adversaries.

The cybersecurity industry has developed multiple naming systems for threat actors, each grounded in unique vantage points, intelligence sources, and analytic rigor. These taxonomies provide critical adversary context to help organizations understand the threats they face, who is targeting them, and why. But as the adversary landscape grows, so does the complexity of cross-vendor attribution. Through this deeper collaboration, CrowdStrike and Microsoft have developed a shared mapping system – a 'Rosetta Stone' for cyber threat intelligence – that links adversary identifiers across vendor ecosystems without mandating a single naming standard.

By reducing ambiguity in how adversaries are labeled, this mapping enables defenders to make faster, more confident decisions, correlate threat intelligence across sources, and better disrupt threat actor activity before it causes harm. By making it easier to connect naming conventions like COZY BEAR and Midnight Blizzard, the mapping supports quicker decision-making and unified threat response across taxonomies.

"This is a watershed moment for cybersecurity. Adversaries hide behind both technology and the confusion created by inconsistent naming. As defenders, it's our job to stay ahead and to give security teams clarity on who is targeting them and how to respond. This has been CrowdStrike's mission from day one," said Adam Meyers, Head of Counter Adversary Operations at CrowdStrike. "CrowdStrike is the leader in adversary intelligence, and Microsoft brings one of the most valuable data sources on adversary behavior. Together, we're combining strengths to deliver clarity, speed, and confidence to defenders everywhere."

The collaboration will start with a shared analyst-led effort to harmonize adversary naming between CrowdStrike and Microsoft's threat research teams. Through this collaboration, the companies have already deconflicted more than 80 adversaries, including validating threat actors like Microsoft's Volt Typhoon and CrowdStrike's VANGUARD PANDA are Chinese state-sponsored threat actors, and that Secret Blizzard and VENOMOUS BEAR refer to the same Russia-nexus adversary. This demonstrates the real-world value of shared attribution. Moving forward, CrowdStrike and Microsoft will continue working together to expand this effort, inviting other partners to contribute to and maintain a shared threat actor mapping resource for the global cybersecurity community.

"Cybersecurity is a defining challenge of our time, especially in today's AI-driven era," said Vasu Jakkal, Corporate Vice President, Microsoft Security. "Microsoft and CrowdStrike are in ideal positions to help our customers, and the wider defender community accelerate the benefits of actionable threat intelligence. Security is a team sport and when defenders can share and react to information faster it makes a difference in how we protect the world."

This collaboration builds on each company's deep history of threat intelligence leadership and advances a shared mission: delivering better outcomes for defenders by putting customers first and the mission before the market.

To learn more about the CrowdStrike and Microsoft collaboration on cyber threat attribution, please visit our blog.

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/

View source version on businesswire.com: https://www.businesswire.com/news/home/20250602497894/en/

Media Contacts:
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike