CROWDSTRIKE

CrowdStrike Products

Solution Brief

Falcon Adversary OverWatch: Identity Threat Hunting

Disrupt sophisticated adversaries executing identity-based attacks with 24/7 managed threat hunting powered by AI and CrowdStrike expertise

Challenges

Adversaries aren't breaking in, they're logging in. More than half of breaches involve credentials, bypassing traditional endpoint protections to gain access to an organization's network without being detected. According to the CrowdStrike 2024 Global Threat Report, malware-free intrusions represented 75% of detections in 2023.

This trend indicates that adversaries are increasingly employing identity attacks — like phishing and social engineering — and purchasing stolen credentials on criminal forums to gain access. Once they log in, they move quickly, breaking out from the initial system to move laterally within the network. The CrowdStrike 2024 Global Threat Report showed that the fastest eCrime breakout time in 2023 was just over 2 minutes.

Identity is the new security battleground, and the onslaught of identity-related attacks requires constant vigilance. With adversaries' growing proficiency in obtaining legitimate credentials, hunting for users performing unexpected activity has never been more important. Defenders need to stop breaches faster by protecting workforce identities and enforcing multifactor authentication (MFA) when suspicious user activity is detected.

Solution

Identity threat hunting is a complex task requiring expertise and sophisticated tools. CrowdStrike Falcon® Adversary OverWatch™ reduces cost and complexity by delivering a managed service that provides 24/7 protection — all powered by AI and CrowdStrike's unrivaled team of threat hunting experts.

The inclusion of identity data in threat hunting activities is a crucial component of a comprehensive investigation. Adversaries often gain access to numerous accounts to maintain persistent access during an intrusion. CrowdStrike Falcon® Identity Protection generates robust identity telemetry, enabling CrowdStrike's threat hunters to identify both managed and unmanaged hosts. This allows them to detect adversaries attempting to gather additional credentials or escalate privileges in preparation for lateral movement.

Key benefits

- CrowdStrike Falcon® Adversary OverWatch™ **proactively hunts down adversaries across identity, endpoint and cloud** and promptly alerts you, with mitigation steps to stop the intrusion
- CrowdStrike threat hunters **detect the stealthiest adversaries,** including those that use tactics such as brute-force attacks, account takeover, privilege escalation or suspicious login activities from unfamiliar locations or devices
- Falcon Adversary OverWatch tools **constantly monitor the criminal underground** for compromised credentials and mitigate the threat using Falcon Identity Protection

By continuously monitoring user behaviors, access controls and authentication mechanisms, Falcon Adversary OverWatch can detect threats that specifically target user credentials, allowing organizations to undertake proactive mitigation and defensive actions.

Key capabilities

Disrupt identity-based attacks

- **24/7/365 global coverage:** When a sophisticated intrusion occurs, time is critical. Adversaries are not restricted by time zones or geography — and CrowdStrike's threat hunters are always watching.
- **Identify compromised credentials:** Falcon Adversary OverWatch analyzes user identity data, login patterns and authentication data to detect early signs of compromised credentials. This data is used to enrich intrusion investigations with endpoint and cloud runtime telemetry. Upon discovery, Falcon Adversary OverWatch hunters promptly alert customers so they can take immediate action to mitigate the impact of unauthorized access in their environments.
- **Discover stolen credentials on the dark web:** Falcon Adversary OverWatch continuously monitors criminal forums for stolen credentials and will force an MFA challenge or password reset through Falcon Identity Protection.

Hunt identity threats across endpoints and cloud

Identity threat hunting is crucial, as adversaries are increasingly exploiting compromised identities to launch attacks on endpoint and cloud environments. With Falcon Adversary OverWatch, you can gain comprehensive protection across endpoints and cloud environments and peace of mind against sophisticated identity threats.

- **Protection for endpoints:** Falcon Adversary OverWatch threat hunters relentlessly pursue adversaries targeting your endpoints. Fortify your defense against sophisticated identity attacks with real-time protection and accelerated response.
- **Protection for cloud environments (AWS, Azure and GCP):** Leveraging patented cloud-native tooling and tactics, Falcon Adversary OverWatch scours hybrid and multi-cloud environments for identity threats across cloud workloads and infrastructure.

Speed up decision-making with intelligence

- **Adversary insights:** Falcon Adversary OverWatch tracks 230+ nation-state, eCrime and hacktivist adversaries. Identify the adversaries targeting your organization, and gain insights into their intent and capabilities.
- **Automated malware sandbox:** Safely detonate suspicious files in a secure environment. Get threat verdicts, severity ratings and indicators of compromise (IOCs), and understand file behavior and related malware to anticipate and stop future attacks.
- **Context-aware indicators:** CrowdStrike Falcon® platform modules are enriched with built-in intelligence and context-aware indicators. Explore the relationship between IOCs, endpoints and adversaries, and search across millions of real-time threat indicators.

Examples of Falcon Adversary OverWatch identity threat hunting

- **Malicious access:** During an eCrime intrusion, a Falcon Adversary OverWatch threat hunter discovered 21 compromised accounts attempting to log in from a malicious VPN. Upon investigating a known compromised user, the hunter detected logins from unknown IP addresses. It was also observed that the other 20 users had logged in or attempted to log in from the same IP. Recognizing the malicious nature of this activity, the analyst quickly notified the customer, enabling them to immediately reset the password and block the malicious IPs.
- **Multi-domain attack:** A Falcon Adversary OverWatch threat hunter used both identity and endpoint data to inform their analysis while hunting an eCrime intrusion. The analyst was able to understand the adversary's identity reconnaissance efforts, the tools they used on the endpoint and their credential dump attempts. Due to this comprehensive insight, the customer rapidly disabled the compromised accounts and contained the intrusion.
- **Identity attack on the cloud:** During an eCrime intrusion, a Falcon Adversary OverWatch threat hunter used data from CrowdStrike Falcon® Cloud Security to support the analysis. The analyst identified the adversary's attempt to establish persistence in the cloud by adding an additional federated domain. Such visibility would not have been possible with cloud data alone. In this instance, the analyst provided essential intelligence that enabled the customer's incident response team to quickly contain the incident.

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/

Attend a hands-on workshop →

Request a demo →