

# FALCON INTELLIGENCE RECON

Prevent dark web threats that can compromise identities, steal sensitive data and destroy your organization's brand

## STOP CYBERCRIMINALS IN THEIR TRACKS

CrowdStrike Falcon® Intelligence Recon provides security teams with deep visibility into the cybercrime activities unfolding on the dark web and enables them to reduce the risk to their organization. Real-time dark web monitoring with integrated response workflow empowers security analysts to discover and disrupt threats that have the potential to target employees, steal sensitive data and cause lasting brand damage.

## KEY CAPABILITIES

### MONITOR THE DARK WEB FOR THREATS

Falcon Intelligence Recon provides multiple levels of threat visibility outside the traditional perimeter and gives security teams the opportunity to stop threats before they turn into a major breach. Users are able to:

- **Access real-time raw intelligence:** Safely scan hundreds of underground criminal forums, marketplaces and underground communities. Falcon Intelligence Recon archives historical threat data so adversaries can't cover their tracks by changing or deleting posts.
- **Discover domain impersonations and exposed credentials:** Uncover fraudulent domain registrations that adversaries use to launch phishing attacks and deliver malicious content. Discover leaked organizational data and credentials — even those not yet for sale.
- **Identify targeted threats:** Detect imminent external threats in real time across criminal forums, marketplaces and underground communities with easy-to-use monitoring rules that include predefined search criteria such as brand names, executives, domains, vulnerabilities, email addresses and many more. Create and save your own monitoring rules so you can proactively sift through raw intelligence.

## KEY BENEFITS

Broad visibility covering hundreds of criminal forums and marketplaces

Real-time dark web scanning with easy-to-use rules tailored to your organization

Summarized exploit and actor threat context to prioritize and filter vulnerabilities

Early warning on domains impersonating the organization and related brands

Instant time-to-value — deploys and is operational in minutes

Support for multiple threat use cases — because threat actors don't stay in their lane

## FALCON INTELLIGENCE

### UNDERSTAND THREATS THAT MATTER

Falcon Intelligence Recon shines a light on global criminal underground activities, as well as the monikers behind them, and enriches traditional vulnerability management with new context to maximize risk mitigation efforts. With this, you can:

- **Know your adversary:** Review actor profiles using the MITRE ATT&CK® framework. Investigate threat actors' tactics and techniques with a single click.
- **Follow cybercriminals' steps:** Review underground posts by filtering for "author handle" and site statistics. Results are viewed in their original language and can be translated from 18 other languages using augmented translation, complete with hacker slang dictionaries.
- **Gain vulnerability Intelligence:** Prioritize attack surface mitigation efforts based on exploits seen in the wild. Falcon Intelligence Recon allows users to filter through thousands of vulnerabilities by exploit status and related actors, vendors and products.
- **Access cybercrime reports:** Get weekly reports about novel underground activities and the latest cybercrime news. Learn important information about key eCrime trends related to ransomware campaigns, access broker activity, vulnerability exploits and more.

### DISRUPT IMMINENT THREATS

Expand detection, investigation and response workflows with real-time alerts on external threats. Ensure the users responsible for triage, investigation and response have the details they need at their fingertips. With Falcon Intelligence Recon, you can:

- **Receive actionable alerts:** Easy-to-use wizards help set up monitoring of organization-specific digital assets, brand names, executives, domains, vulnerabilities and more. Configure the priority of each alert and immediately pivot from the notification to the critical details.
- **Drill down:** Review exposed data such as user names, passwords, organizational asset details and confidential data. Examine discovered malicious domain details including IP name servers, MX records, SSL certificates and Whois records.
- **Alert the right teams:** Digital threats affect an organization's brand, reputation and employee safety. Go beyond cybersecurity and alert departments such as marketing, legal, human resources and fraud. Integrate this information into third-party ticketing systems, SIEMs and SOARs via easy-to-use REST APIs

## EDITIONS

Falcon Intelligence Recon is available in two editions:

- **Falcon Intelligence Recon Enterprise:** Track adversaries and their activities and exploits outside the perimeter:
  - Monitor the criminal underground and scan for external attack vectors
  - Identify exposed confidential data and domain impersonations
  - Access vulnerability intelligence, adversary profiles and cybercrime activity reports
  - Assign and manage alerts. Use REST APIs for easy integration into third-party solutions
- **Falcon Intelligence Recon+:** includes everything in Falcon Intelligence Recon Enterprise, with the additional benefit of having CrowdStrike experts manage everything for you.

## DIGITAL RISK RECON USE CASES

**Threat awareness:** Falcon Intelligence Recon provides periodic reports about nefarious activities on criminal underground

**Brand abuse:** Discover activities associated with domain impersonations and other fraudulent interactions affecting your brand

**Vulnerability intelligence:** Filter through thousands of vulnerabilities by exploit status, related actor, vendor and products

**Exposed data discovery:** Detect compromised credentials and the theft of sensitive data, including IP and credit card information, by scanning data leaked on criminal forums and exposed during breaches

**Supply chain monitoring:** Falcon Intelligence Recon helps identify threats to your suppliers by exposing chatter, phishing campaigns, counterfeit websites and more

**Executive protection:** Falcon Intelligence Recon monitors threats, impersonations and phishing attempts against VIPs and executives don't stay in their lane



## FALCON INTELLIGENCE

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

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

2023 CrowdStrike, Inc. All rights reserved.

