FLASHPOINT

Compromised Credentials Monitoring: The Flashpoint Advantage

Flashpoint Compromised Credentials Monitoring (CCM) allows users to monitor exposure of compromised credentials for their employee and customer email addresses to take action after breaches to mitigate risk of account takeover (ATO).

Expansive Data Collections

Flashpoint provides the largest source of stolen and leaked credentials obtained from open web and illicit communities, as well as closed, invitation-only sources, such as forums, chat services, and marketplaces.

- **First Access to Breach Data:** Ability to track adversaries across multiple types of online communities uniquely positions the company to engage with threat actors directly and procure compromised assets before breaches occur.
- **Robust Collections:** Scales breaches and leaks of all magnitudes, providing broader insight into the credential landscape, which includes thousands of automated and manually sourced breaches processed within Flashpoint's collections since 2011.
- **Unique Sources:** Flashpoint's access to top tier communities provides insight into private threat actor discussions and technical data - such as credential stealing malware, and private leaks ensuring signal-rich data.

8.5 BILLION +
Unique credentials in Flashpoint's dataset based on email/password combinations

40 BILLION+
Compromised credentials collected by Flashpoint from 2011 to present

Trusted Intelligence Program

Flashpoint intelligence analysts have spent years monitoring illicit communities, and are armed with the skill sets to know when and where compromised databases and credentials are exposed.

EXPERIENCED INTELLIGENCE PROFESSIONALS

Our analysts' familiarity operating in threat actor communities and with actor tactics, techniques and procedures (TTPs) enables them to identify recycled data leaks advertised as new leaks, and ensure customers are provided the most relevant and recently compromised credentials.

ADDRESS INTELLIGENCE REQUIREMENTS

Flashpoint credential data enables users to conduct more than just a tactical reset; our data enrichment, contextual insights, and RFI service support your team's ability to conduct sensitive investigations or research into campaigns, emerging actors or TTPs in support of your intelligence requirements.

Advanced Processing & Technology

Fueled by sophisticated technology and collections, Flashpoint quickly collects and processes data and credentials, allowing for organizations to access the most up-to-date breach data and receive notification as soon as credentials have been identified.

- **Filter Out Recycled Credentials:** Internal teams receive newly compromised accounts, without the delay of sifting through recycled credentials.
- **Seamless API Integration:** Teams can take immediate action on compromised assets by integrating Flashpoint's API into their existing business processes, saving both analyst time and resources.

ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams—rely on the Flashpoint Intelligence Platform, comprising open-source (OSINT) and closed intelligence, to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

Learn more at flashpoint.io.