FLASHPOINT

Compromised Credentials Monitoring: Enterprise

Abuse of enterprise credentials allows attackers onto your network and exposes sensitive business and personal data. Compromised Credentials Monitoring - Enterprise enables organizations to search and monitor Flashpoint's unique collections for compromised enterprise accounts and passwords in order to flag accounts, reset employee passwords, and restrict permissions to prevent actors from accessing confidential or personally identifiable information (PII). Flashpoint's ability to filter out compromised email addresses that do not meet an organization's password requirements, or identify only data from recent and relevant breaches, allows users to receive alerts on actionable data, saving time and resources.

Key Benefits

- Monitor domains related to the organization, including subsidiaries
- Safely access Flashpoint's collections, and conduct in-depth searches for recently disclosed and historical breaches against Flashpoint's archive of compromised credentials
- Easily explore stolen credentials and track changes over time with the ability to analyze a breach
- Filter out false positives for compromised email addresses that do not fit an organization's password requirements
- Seamless integration via the Flashpoint API

Use Case

PREVENTING ACCOUNT TAKEOVER (ATO)

Employee reuse of passwords, where the same or similar passwords and email addresses are recycled for different web-based services, presents a major risk to enterprises. Knowing this tendency, threat actors who compromise or gain access to leaked credentials will use them to gain access to numerous enterprise networks or web-based services.

- **Restrict User Access & Know When to Reset Passwords**
  Flashpoint's system can filter false positives and provide organizations with the compromised credentials that meet their organization's password policy. This is a critical step enabling enterprises to take action against alerts. Companies may leverage Flashpoint's API and data to automate workflows to reset exposed employee credentials, restrict access to resources, or receive notification when a compromise has been detected.

- **Enforce Strict Password Policy**
  Flashpoint Compromised Credentials Monitoring - Enterprise provides the ability to search through Flashpoint's historical compromised credentials collections to view password data, as well as their complexity based on length, upper-case letters, numeric, and special characters. Users are able to create password profiles to see how many passwords would have been filtered out based on the complexity requirements. This provides insight and helps organizations understand an enterprise's exposure and how complex their exposed passwords are, arming customers with data in order to support the enforcement of password complexity requirement policies, thereby mitigating risk to the organization.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**