FLASHPOINT

Flashpoint for Public Sector

Actionable intelligence on adversaries operating within illicit online communities is indispensable in support of many missions. Access to information on terrorist activity and recruitment, the spread of jihadi propaganda, cyberattacks, fraudulent activity, malicious insiders, supply-chain threats, and more is difficult and, in some instances, could be dangerous to obtain.

Without the necessary expertise and technology to automate secure and persistent data-gathering within closed-source and vetted areas of the predominantly unindexed internet, attempting to gather this information results in gaps in intelligence and creates additional risk to a collections team. Here's how Flashpoint empowers and supports public sector requirements and missions:

Flashpoint Intelligence Platform grants access to our archive of finished intelligence reports, data from illicit online sources, compromised credentials from data breaches, and risk intelligence observables in a single, finished-intelligence experience. Key features include a universal search for all Flashpoint illicit community data, intuitive pivoting from reports into a sanitized copy of threat-actor conversations, and translated conversations, enabling native language content from illicit communities in English within the platform. Flashpoint's datasets include:

- **Finished Intelligence:** Access to analytical reports produced by our intelligence analysts that cover illicit underground activity, including violent extremism, and physical threats.
- **Forums:** Access to signal-rich discussions from illicit threat-actor communities supplements and complements internal data with targeted data from highly curated sources.
- **Risk Intelligence Observables (RIOs):** A high-fidelity feed of cyber observables. RIOs integrate with security operations to enrich user data with additional context.
- **Technical Indicators:** Access to indicators of compromise (IOCs) and technical data across Flashpoint datasets.
- **Paste Sites:** Enables access to openly shared research, data leaks, and other plain text files frequently used by anonymous sources and threat actors to share malicious activity, providing a broader view into open web data.
- **Card Shops:** Users are provided credit card data including BIN numbers, country location, and expiration dates within these collections of stolen payment card data found in illicit high-end credit card shops.
- **CVE:** Access to the latest CVEs within Flashpoint collections, including access to MITRE and NVD data, as well as CVEs discussed by threat actors as observed by Flashpoint intelligence analysts and embedded technologies.
- **Blogs:** A view into online sources of news and information related to threat actors and collectives, allowing users to comprehensively monitor activity in malicious communities, as well as risks impacting the organization.
- **Account Shops:** Identify compromised accounts found for sale in illicit account shops, further stifling the risk of employee or end-user login details being used in credential stuffing attacks.
- **Marketplaces:** Access to top-tier marketplaces, where threat actors buy and sell items such as stolen credentials and personally identifiable information (PII).
- **Chat Services:** Access to around-the-clock conversations within threat-actor channels to monitor and gain insights across threat-actor communities. Collections include Telegram, Discord, as well as Chinese-speaking threat actors.
- **Message Boards:** Access to these anonymous message boards, enabling users to monitor malicious content and discussions ranging from hacktivism to physical threats.
- **Compromised Credentials:** Allows users to monitor exposure of compromised credentials for their employee and potential end-user email addresses to take action after breaches to mitigate risk of account takeover (ATO).

Subject Matter Expertise:
Flashpoint has recruited industry veterans who help shape and drive the strategy of the company. The Flashpoint team is composed of former intelligence practitioners from the public sector including: Department of Homeland Security, FBI, The White House, UK Government, among others. This experience helps shape Flashpoint's client success, collections, and overarching needs to address the most critical problems these entities face.

Alongside these team members, Flashpoint analysts know what data to collect, have the agility to move collections capabilities to go where adversaries go, and can rapidly analyze, refine, and contextualize that data to produce trusted intelligence.

Capabilities include:

- Tradecraft honed over years of operating in the most austere online environments and training in elite government and corporate environments
- Already embedded in these communities for years with redundant layers of access
- Intimate understanding of cultures and communities
- Multilingual capabilities in more than 20 languages with textured understanding of vernacular and slang

BELOW ARE EXAMPLES OF USE CASES SUPPORTED BY FLASHPOINT:

Terrorism/Extremism
Flashpoint has been consistently and discretely tracking Al-Qaida, ISIS, and other organizations predating 9/11 to the first instances of these groups using the internet for recruitment and propaganda. Our data collections extend to that time period, and our finished intelligence supports a number of government and law enforcement missions:

- **Counterterrorism, Propaganda and Recruitment:** Access to Flashpoint data provides early insight to extremist recruitment and propaganda dissemination before it reaches a larger audience.
- **Physical Security:** Intelligence analysts responsible for protecting against physical threats leverage data collected from illicit communities to follow threat actors or terrorist groups, and understand the scope and scale of threats.
- **Force Protection:** Teams supporting personnel security have timely access to intelligence to the TTPs of online Jihadist communities weaponizing drones, constructing IEDs and targeting military personnel.

Cyber Intelligence
Flashpoint provides extensive and timely access to illicit communities including closed, invite-only, and password-protected sources, as well as paste sites, technical data, indicators of compromise, and stolen credentials exploited by illicit communities.

- **Malware:** Threats such as ransomware or malicious code that targets credentials and personally identifiable information puts agencies at risk. Access to discussions and development of unreleased malware can be leveraged before campaigns are deployed.
- **Exploits:** Known and previously unknown vulnerabilities are often discussed in closed-source illicit communities, where exploit code is also developed and shared. Flashpoint data puts this information within reach before exploits are delivered at scale.
- **Nation-States:** State actors strategically aim for high-value targets. Flashpoint's visibility into illicit communities provides analysts with insights into these campaigns and tools.

Fraud and Insider Threats

Flashpoint informs on emerging trends that affect Federal Civilian Agencies and law enforcement programs. Our unique position to glean information from the open web and closed-source illicit communities allows us to incorporate differentiated, signal-rich, unclassified data into our analysis, and provide access to primary sources, supporting the following:

- **Entitlements Fraud:** Threats to entitlement programs and the personally identifiable information of participants is often discussed or developed with communities monitored and collected by Flashpoint. Access to these insights and discussions helps decision makers create and implement new policies to reduce fraud.
- **Narcotics:** Promotion and sale of opioids, pharmaceuticals, and other narcotics are seen on Illicit forums and marketplaces. Access to Flashpoint's extensive dataset enables law enforcement to identify sellers, behaviors, and products to help understand distribution channels and financial impact.
- **Compromised PII:** Stolen personally identifiable information (PII) is often sold within illicit communities for the purposes of creating false forms of identification, such as driver licenses and passports.
- **Financial Crime:** Uncovering the methods used to recruit money mules and target financial institutions is critical to stopping this fraudulent activity. Leveraging insights from illicit communities allows law enforcement teams to also identify and inform compromised financial institutions.
- **Supply Chain:** The integrity of the supply chain remains a critical risk area that must be managed for a number of threats, including interdiction, counterfeit or vulnerable software, or rogue services that could impact confidentiality or availability.

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.

Learn more at https://www.flashpoint-intel.com/.