FLASHPOINT

PUBLIC SECTOR

FLASHPOINT FOR DEFENSE & INTELLIGENCE

Defense and Intelligence agencies require reliable, actionable intelligence in support of their operations. Access to online illicit communities are a key and necessary source for critical intelligence in support of a variety of operations. Access to information on terrorist activity, the spreading of jihadi propaganda, terrorist recruitment, and other threat actors is difficult and dangerous to obtain. Without the necessary expertise and technology to automate secure and persistent data-gathering within these illicit communities, attempting to gather such information results in gaps in intelligence and creates additional risk to the intelligence collections team.

Flashpoint offerings align to every step in the intelligence cycle; by monitoring and identifying publicly available closed source and vetted communities of interest in support of intelligence needs and collection requirements. Flashpoint's unique access to illicit online communities, enables intelligence teams to perform further analysis, and produce intelligence in support of their mission.

SOLUTION

Flashpoint is able to access, monitor, and engage in illicit communities, enabling the ability to provide finished intelligence reports which detail activities and trends derived from these communities in support of intelligence operations.

Flashpoint Intelligence Platform

OVERVIEW

Flashpoint Intelligence Platform grants access to our expansive archive of Finished Intelligence reports, Illicit Forums, Illicit Marketplaces, Risk Intelligence Observables (RIOs), and Chat Services, in a single, finished intelligence experience. Our platform scales Flashpoint's internal team of specialized, multilingual intelligence analysts' ability to quickly provide responses to customers.

KEY FEATURES

Finished Intelligence: Access both our Finished Intelligence reports and primary source data used by our experts to create those reports.

Universal Search: Search all of Flashpoint's illicit community data safely and gain greater context around any information a customer might need.

Intuitive Pivoting: Browse or search reports, then pivot directly into a sanitized copy of the original threat actor conversation.

Flashpoint Datasets

Finished Intelligence: Analytical reports produced by our Subject Matter Experts (SMEs). Reports cover a wide spectrum of illicit underground activity, from crimeware to fraud, emergent malware, violent extremism, and physical threats.

Forums: Access to our extensive historical archive of signal-rich discussions from DDW threat actor communities. This data enables users to leverage illicit online communities safely and supplement their internal data with targeted data from highly curated sources affording users with a strategic advantage over adversaries.

Marketplaces: Access to top-tier marketplaces, where threat actors buy and sell items such as stolen credentials and personally identifiable information (PII), providing users the ability to search and filter by items, source, vendor, and price.

RIOs: A high-fidelity feed of cyber observables. RIOs integrate with security operations to enrich user data with additional context and provide visibility into activities and events extending beyond indicator-based datasets.

Chat Services

Access to Chat Services is available through the Flashpoint Intelligence Platform, and provides organizations access to around-the-clock conversations within threat actor channels to monitor and gain insights across threat actor communities. These conversations provide insight into a broad spectrum of illicit activity, threat actor tactics, techniques, and procedures (TTPs), and the distribution of propaganda. Chat Services provides additional insights for security teams to discover and respond to threats in a timely manner.

USE CASES

Counterterrorism - Propaganda and Recruitment: Chat service platforms have been established as a tool for extremist recruitment and followers, as well as the initial medium to deliver propaganda before it is disseminated through other means. Access to Flashpoint Chat Services provides users early insight to official communication and discussions, before it reaches a larger audience.

Physical Security: Terrorist groups leverage chat service platforms as a means to expand their footprint and to encourage individuals to self-radicalize, resulting in acts of terrorism. Intelligence analysts responsible for protecting against physical security threats leverage illicit online communities and Chat Services to follow threat actors or terrorism groups, monitoring the conversations and users in near real time to understand the scope and scale of the threat.

Force Protection: Online Jihadist communities share TTPs related to weaponizing drones, the construction of IEDs, and targeting of military personnel. Teams in charge of supporting the security of their personnel, need timely access to intelligence, providing a thorough understanding of new TTPs, and how terrorists are targeting their teams.

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. Flashpoint is backed by Georgian Partners, Greycroft Partners, TechOperators, K2 Intelligence, Jump Capital, Leaders Fund, Bloomberg Beta, and Cisco Investments.