FLASHPOINT

PUBLIC SECTOR

FLASHPOINT FOR FEDERAL CIVILIAN AGENCIES

The Deep & Dark Web (DDW) is a key source for critical intelligence on illicit communities in support of fraud, financially motivated cyber crime, money laundering, and risks directly to the agency.

Access to information on cybercriminals and other threat actors in the DDW is difficult and dangerous to obtain. Without the necessary expertise and technology to automate secure and persistent data-gathering within the DDW, Federal Agencies attempting to gather such information creates substantial risk for their employees.

Flashpoint informs decision makers on emerging trends that affect policy and threats to Federal programs. Our unique position to glean information from the DDW allows us to incorporate highly differentiated and signal-rich, unclassified data into our analysis, as well as provide access to primary sources.

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 the DDW in support of policy and regulatory responsibilities.

Flashpoint Intelligence Platform

OVERVIEW

Flashpoint Intelligence Platform grants access to our expansive archive of Finished Intelligence reports, DDW Forums, DDW Marketplaces, 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.

DDW Search: Search all of Flashpoint's DDW 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 SMEs. Reports cover a wide spectrum of illicit underground activity, from crimeware to fraud, emergent malware, insider threat, violent extremism, and physical threats.

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

DDW 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.

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, thereby reducing risk to the organization.

USE CASES

Fraud Targeting Entitlement Programs: Threat actors communities provide a location for discussing and developing techniques to bypass security checks against entitlement programs, such as medicare and social security. Increasingly, chat services platforms are used to quickly support fraudulent activities, due to the nature of the live conversations within those platforms. Access to these insights and discussions help policy makers create and implement new policies to reduce fraud. Additionally, it provides information that can support audits of entitlement programs and uncover those who are committing fraud.

Cyber Threats to the Agency: Ransomware has become a threat vector for threat actors to target individuals who have access to proprietary or sensitive information. Actors discuss the development of unreleased malware within the DDW. By tracking this activity, Flashpoint is providing the indicators of compromise (IOCs) and collecting observables, identifying who is producing the malware along with where and how the development was taking place. Cybersecurity teams leverage this intelligence to be prepared to combat the malicious campaign before it becomes widely deployed.

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.