Enhanced Monitoring Service

Threat actors constantly evolve their methods of extorting information and payments from victims. Attacks like ransomware, distributed denial-of-service (DDoS), or executive targeting, often result in sensitive information and assets being posted to public repositories. This evolving attack landscape highlights the need for extortion victims, incident response teams, and digital forensics teams to have insight into illicit communities and websites to identify potential exposure via third-party vendors. Teams need to swiftly identify and access relevant breached data in order to adapt and optimize internal response plans.

Overview

Powered by our extensive, signal-rich collections and alerting engine, Flashpoint's Enhanced Monitoring Service delivers real-time automated alerts of identified leaked assets as a result of an extortion incident, providing teams with the necessary insight into the extent of exposure and damage.

Key Benefits

✓ **Continuous Monitoring**

In the event of a breach, stolen data could end up on illicit markets months or years after the initial compromise has occurred—potentially leading to legal ramifications and reputation damage. Enhanced Monitoring provides pre-and post-event keyword monitoring based on your requirements, to continuously assess reputation and legal obligations beyond the conclusion of an investigation or incident response.

✓ **Experienced Experts and Collections**

Flashpoint's multidisciplinary intelligence analysts speak over 35 languages and drive our global collections engine which accounts for our extensive collection of illicit communities. Our data and collections cover more regions, countries, and types of threat actors than our industry peers.

Real Time Alerts

Flashpoint's automated alerting matches conversations from illicit online communities with keywords associated with the team's areas of concern and automatically provides these matches to our intelligence team for further review. The relevant findings are provided to your team for any further action.

Leaked Data Capture

If Flashpoint identifies leaked assets during this monitoring, at your team's request, Flashpoint will attempt to download the data directly from these illicit communities and securely provide it to your team.research or analyze an incident.

Use Cases

When an organization's network is attacked, incident response teams need to assess the intrusion's scope and quickly identify sensitive data exfiltration by the attacker... Enhanced Monitoring helps by notifying teams of leaked data, saving time and resources. Flashpoint provides context around the threats so that immediate action can be taken to mitigate further risk. Our post-incident support ensures that internal teams have the tools and resources they need for continued protection.

Early Warning of Cyber Attacks
Identifying potential threats or vulnerabilities that could be exploited for extortion.

Pre and Post-Attack Monitoring
Monitoring online communications and illicit communities for signs of an impending attack or evidence of a successful breach.

Reputation Management
Monitoring for signs of leaked or stolen data that could be used for extortion or blackmail.

Brand Protection
Identifying instances of brand impersonation or abuse that could be leveraged in extortion schemes.

About Flashpoint

Flashpoint is the leader in threat data and intelligence. We empower mission-critical businesses and governments worldwide to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives.

Discover more at flashpoint.io

Get a Demo