FLASHPOINT

Domain Monitoring

Provides teams the ability, resources, and insight into observed domain phishing activity related to the organization in order to eliminate threats such as typosquatting, phishing attacks, and brand impersonation through logo detection.

Key Benefits

- **ACTIONABLE ALERTS WITH CONTEXT**
  Receive notification of malicious URLs targeting an organization and its affiliated brands with the necessary context to know whether to action a takedown

- **INVESTIGATION OF URL INCIDENTS**
  Analysts investigate and review potentially malicious URLs on your behalf in order to minimize false positives

- **SEAMLESS BRAND MANAGEMENT**
  Centrally manage all your brands and logos within the Flashpoint Intelligence Platform

- **TRACK INSIGHTS RELATED TO THE ENTERPRISE**
  Analyze attacks on your organization's brands to determine which are at highest risk

1 in every 8 employees shares sensitive information on a phishing site

96% of all targeted phishing attacks are intended for intelligence-gathering

SOURCE: https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/#:~:text=1%20in%20every%208%20employees,than%2018%20years%20of%20age

Use Cases

PROTECT AGAINST PHISHING ATTACKS; IDENTIFY AND STOP BRAND IMPERSONATION

Cybercriminals continue to seek creative ways of manufacturing phishing pages to appear legitimate, including stealing company logos and other trademarked information in order to prompt unsuspecting users to enter sensitive information such as passwords or credit card numbers. Flashpoint's ability to identify stolen logos or visuals provides brands the ability to uncover actors and infrastructure impersonating brands for malicious gain, enabling internal teams to swiftly identify pages and take action.

SUPPORT INTERNAL CTI TEAMS; UNCOVER PHISHING SITES AND REMEDIATE THE THREAT

As the threat of phishing attacks continue to increase and grow in creativity as well as levels of sophistication, internal CTI teams struggle to keep up with uncovering and taking down malicious websites. They require support and immediate notification into how the organization and affiliated brands are being targeted, as well as associated context around the threat. Flashpoint provides immediate notification of phishing sites via direct alerts to teams, as well as a one-click option to takedown the site. Once the site is removed, the Flashpoint Intelligence Platform provides the ability for users to continue to monitor and search within our signal-rich collections to further identify threats related to the organization.

ABOUT FLASHPOINT

Trusted by governments, global commercial companies, and educational institutions, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including cyber threat intelligence (CTI), vulnerability management, DevSecOps and vendor risk management teams—rely on the Flashpoint Intelligence Platform to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

For more information, visit **flashpoint.io** or follow us on Twitter at **@FlashpointIntel**