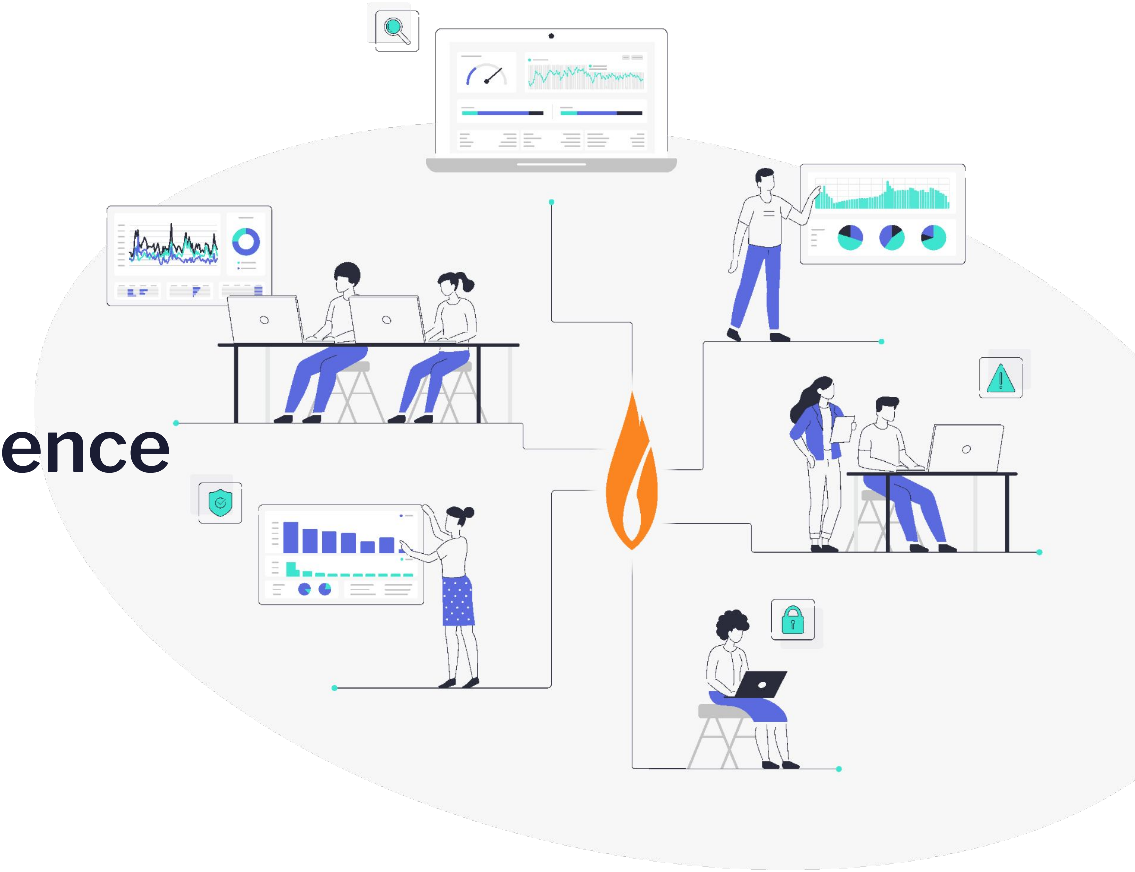
FLASHPOINT

Mitigate risk with personalized intelligence for every team



Organizations face an ever increasing list of challenges

13% increase in ransomware attacks year over year

46% of organizations experienced fraud over last two years

33% known vulnerabilities are not reported by CVE and NVD

40% of data breaches caused by stolen credentials

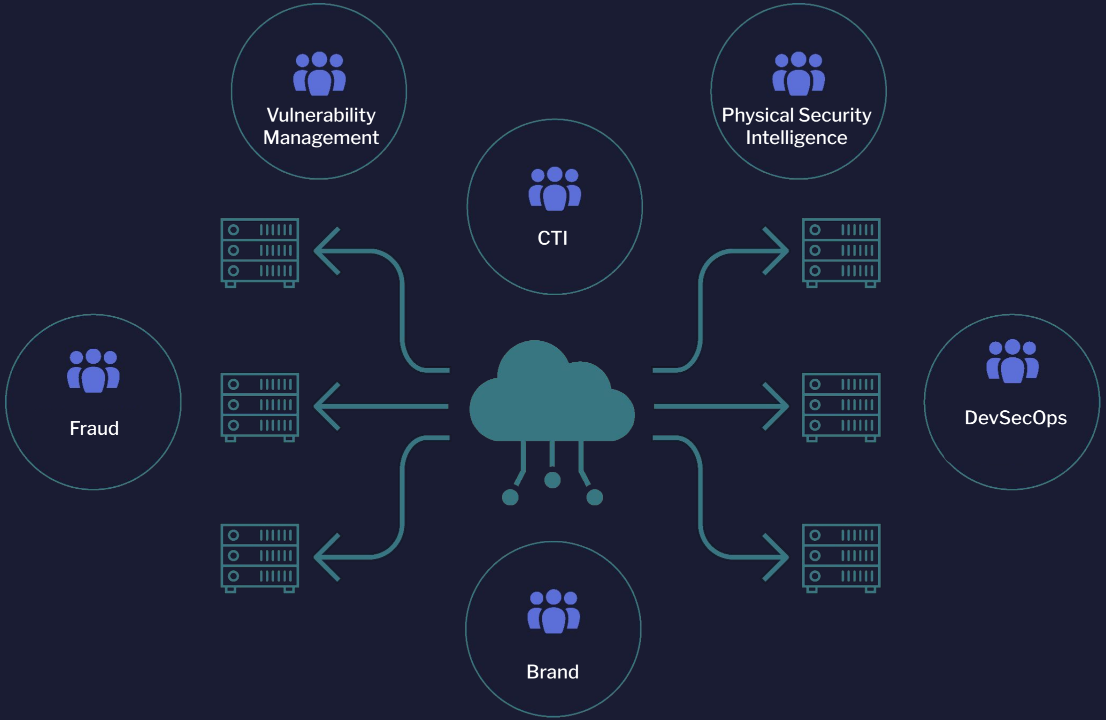
69% of organizations that experienced physical harm to employees/customers missed digital threats

- Overwhelming volumes of data from disparate sources
- Lack of resources/skills gap
- Increased complexity and cost resulting from multiple vendors/solutions

Sources: 2022 Verizon DBIR, PwC Global Economic Crime and Fraud Survey, Flashpoint research, 2021 Ontic Center Mid-Year Outlook State of Protective Intelligence

Throwing more tools at the problem is not the answer

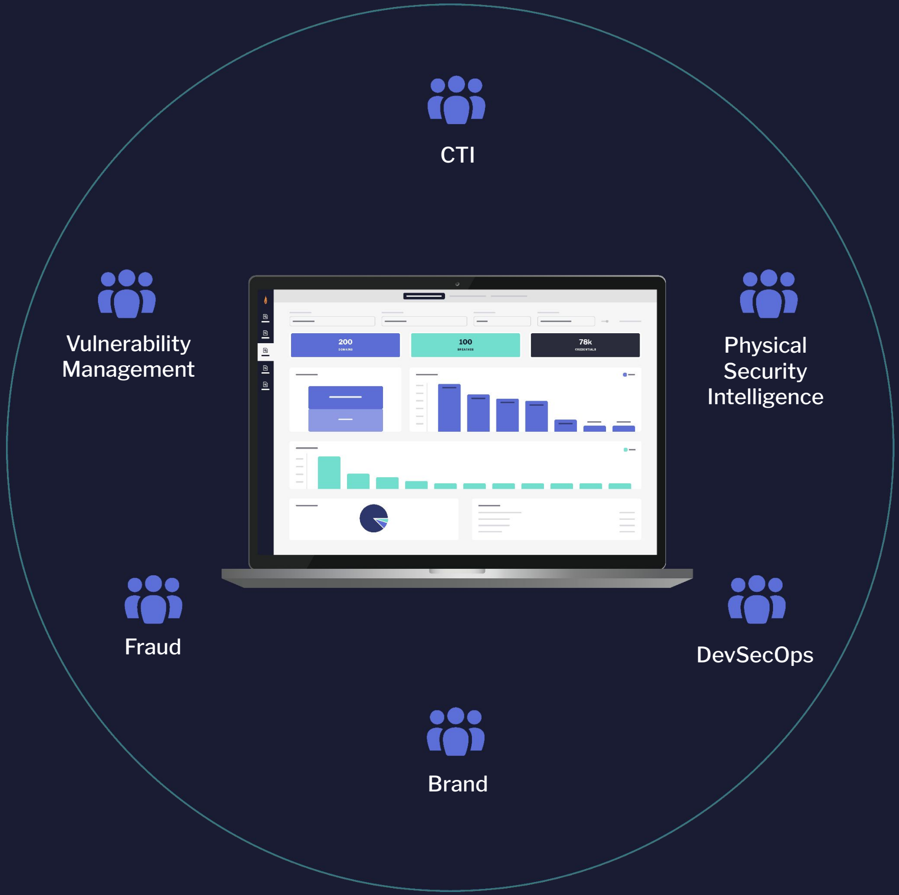
Multiple disjointed feeds and solutions make identifying, prioritizing and mitigating persistent and evolving threats difficult and costly.



FLASHPOINT

Gain a comprehensive view of organizational risk

Automated, multi-source intelligence backed by expert analysts for contextual and actionable intelligence for all teams.



CTI

Vulnerability Management

Physical Security Intelligence

Fraud

DevSecOps

Brand

Who is Flashpoint?

Flashpoint is a risk intelligence company, helping organizations **close the gap between data, intelligence, and action**, to protect their assets and stakeholders.

Intelligence analyst expertise

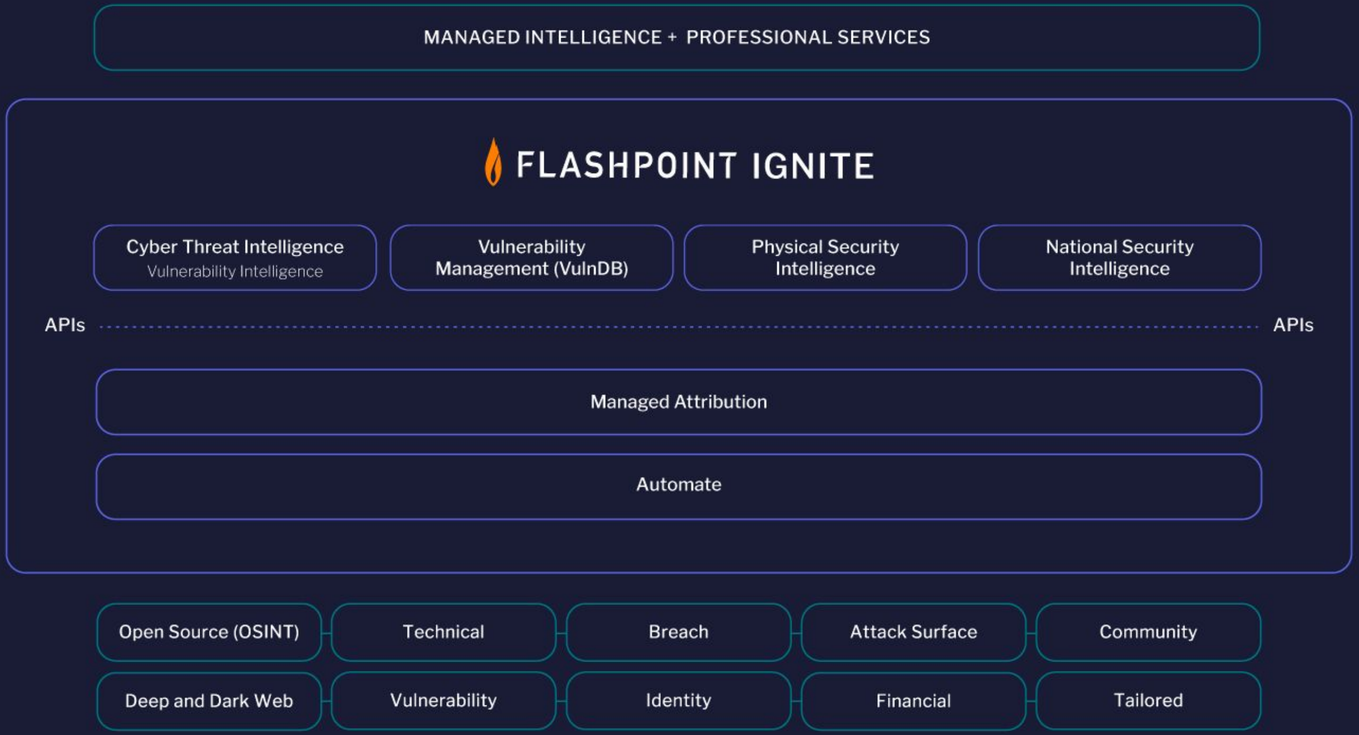
100+ experts who speak 35+ languages

Deep intel and security experience across military, federal, government agencies and Fortune 500s

Diverse backgrounds from intel, malware analysis, compliance, economic policy, risk and counterterrorism

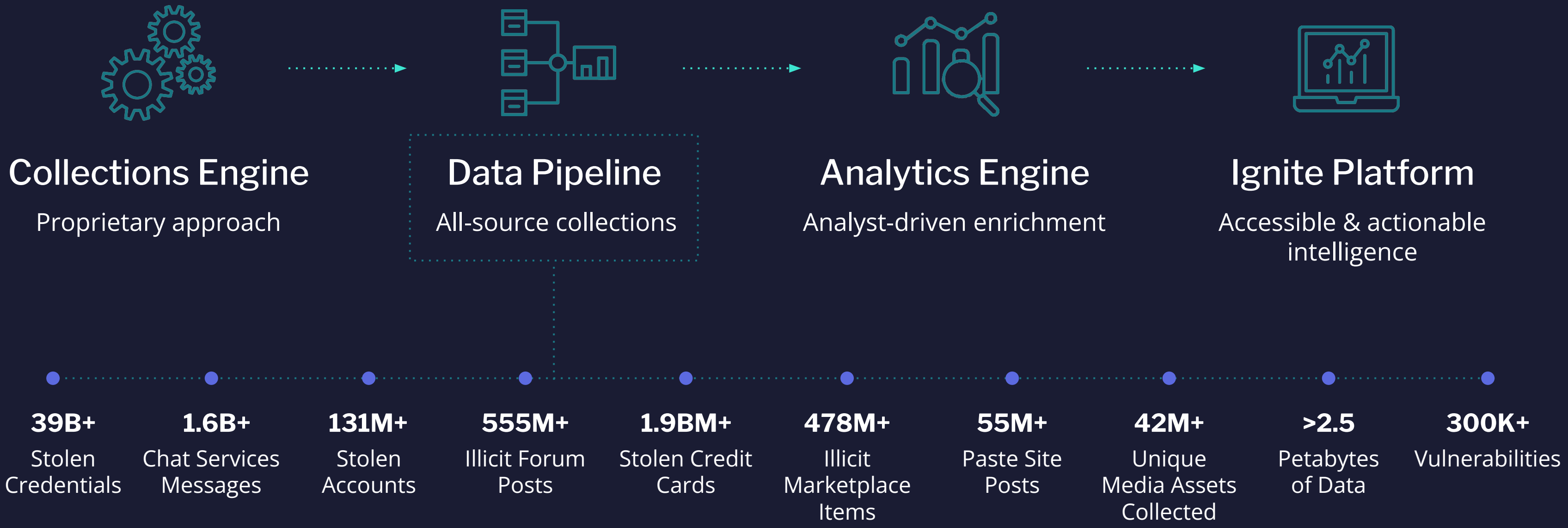
Flashpoint Ignite Platform

A platform of team-based intelligence solutions designed to stop threats and reduce risk across your organization.



MANAGED INTELLIGENCE + PROFESSIONAL SERVICES
FLASHPOINT IGNITE
Cyber Threat Intelligence
Vulnerability Intelligence
Vulnerability Management (VulnDB)
Physical Security Intelligence
National Security Intelligence
APIs
APIs
Managed Attribution
Automate
Open Source (OSINT)
Technical
Breach
Attack Surface
Community
Deep and Dark Web
Vulnerability
Identity
Financial
Tailored

Best-in-class intelligence and advanced analytic tradecraft



Collections Engine

Proprietary approach

Data Pipeline

All-source collections

Analytics Engine

Analyst-driven enrichment

Ignite Platform

Accessible & actionable intelligence

39B+ Stolen Credentials

1.6B+ Chat Services Messages

131M+ Stolen Accounts

555M+ Illicit Forum Posts

1.9BM+ Stolen Credit Cards

478M+ Illicit Marketplace Items

55M+ Paste Site Posts

42M+ Unique Media Assets Collected

>2.5 Petabytes of Data

300K+ Vulnerabilities

Why Flashpoint?

✓ Better Sources

✓ Better Intelligence

✓ Industry Experts

✓ The Most Robust Community

We are obsessed with getting the right information, to the right people, at the right time.

"Our experience with Flashpoint has been excellent from the start and has only gotten better. They provide outstanding intelligence services and support to customers and have an intelligence portal that is constantly being updated with new features.”

–CYBER THREAT TEAM, MANUFACTURING

THE TEXAS A&M
UNIVERSITY SYSTEM

“Flashpoint has allowed us to become more efficient in our investigations and provided us the ability to dedicate more time and focus to complex security challenges.”

–DEPUTY CISO AT TEXAS A&M

482%
ROI

<3 Month
Payback

Net Present Value of $1.9M

Source: Forrester Total Economic Impact™ Study

Recent wins

Flashpoint OCR for cheque fraud

Financial institution saves $10.1 million in one month

Bank sees 93X return on contract value

Flashpoint is trusted by:

swisscom

ATM

AMTRAK

Red Bull ENERGY DRINK

AXA

XL Insurance Reinsurance

Microsoft

Aflac

BlackRock

700+

Clients

50+

Countries

15 / 15

Largest North American Financial Services

30+

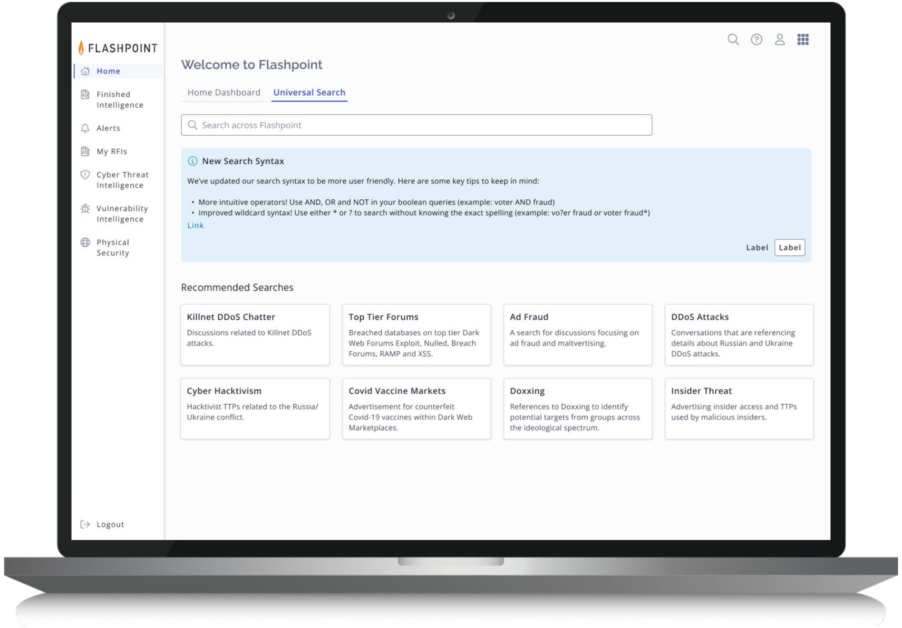
Industries

Appendix

Ignite Platform and Team-tailored Solutions

Flashpoint Ignite Platform

Real-time finished intelligence across multiple teams to improve your organization’s security position



Welcome to Flashpoint

New Search Syntax

We’ve updated our search syntax to be more user friendly. Here are some key tips to keep in mind:

- More intuitive operators! Use AND, OR and NOT in your boolean queries (example: voter AND fraud)
- Improved wildcard syntax! Use either * or ? to search without knowing the exact spelling (example: vo?er fraud *or* voter fraud*)

Link

Recommended Searches

Killnet DDoS Chatter
Discussions related to Killnet DDoS attacks.

Top Tier Forums
Breached databases on top tier Dark Web Forums Exploit, Nulled, Breach Forums, RAMP and XSS.

Ad Fraud
A search for discussions focusing on ad fraud and maltvertising.

DDoS Attacks
Conversations that are referencing details about Russian and Ukraine DDoS attacks.

Cyber Hacktivism
Hacktivist TTPs related to the Russia/ Ukraine conflict.

Covid Vaccine Markets
Advertisement for counterfeit Covid-19 vaccines within Dark Web Marketplaces.

Doxxing
References to Doxxing to identify potential targets from groups across the ideological spectrum.

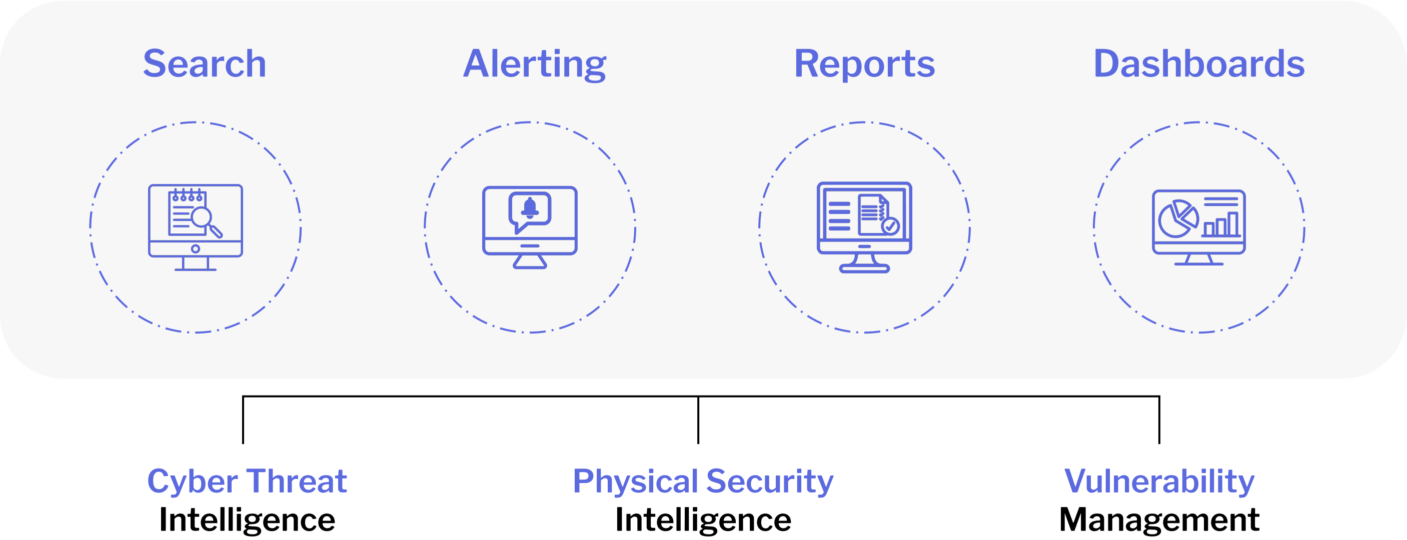
Insider Threat
Advertising insider access and TTPs used by malicious insiders.

Timely and actionable intelligence from thousands of sources with the platform’s integrated product offerings: Cyber Threat Intelligence, Vulnerability Management, and Physical Security Intelligence.

With Ignite you can:

- Achieve more with one platform and seamlessly work across teams
- Access dependable intelligence for everyone
- Close the gap between data, intelligence, and action

Ignite - Key Features



Search

Alerting

Reports

Dashboards

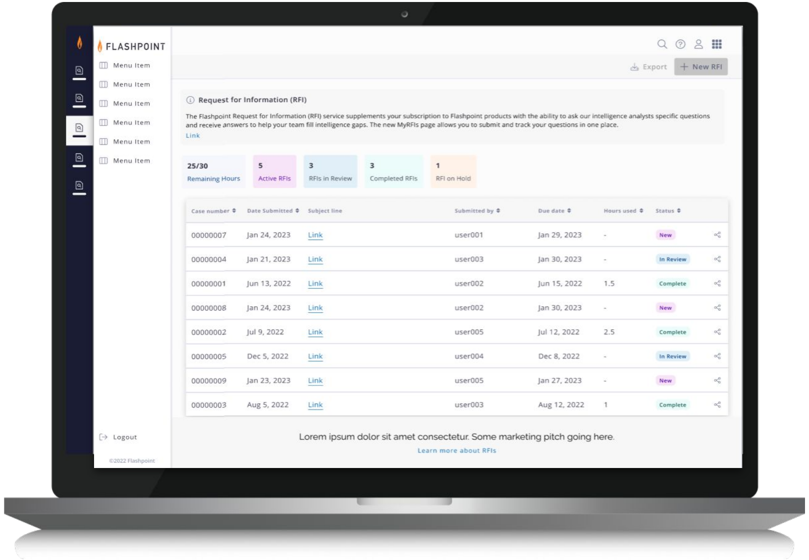
Cyber Threat Intelligence

Physical Security Intelligence

Vulnerability Management

Cyber Threat Intelligence (CTI)

Quickly search across thousands of data sources and curated intelligence to find and respond to threats



Request for Information (RFI)

The Flashpoint Request for Information (RFI) service supplements your subscription to Flashpoint products with the ability to ask our intelligence analysts specific questions and receive answers to help your team fill intelligence gaps. The new MyRFIs page allows you to submit and track your questions in one place.

Link

25/30	5	3	3	1
Remaining Hours	Active RFIs	RFIs in Review	Completed RFIs	RFI on Hold

Case number	Date Submitted	Subject line	Submitted by	Due date	Hours used	Status
00000007	Jan 24, 2023	Link	user001	Jan 29, 2023	-	New
00000004	Jan 21, 2023	Link	user003	Jan 30, 2023	-	In Review
00000001	Jun 13, 2022	Link	user002	Jun 15, 2022	1.5	Complete
00000008	Jan 24, 2023	Link	user002	Jan 30, 2023	-	New
00000002	Jul 9, 2022	Link	user005	Jul 12, 2022	2.5	Complete
00000005	Dec 5, 2022	Link	user004	Dec 8, 2022	-	In Review
00000009	Jan 23, 2023	Link	user005	Jan 27, 2023	-	New
00000003	Aug 5, 2022	Link	user003	Aug 12, 2022	1	Complete

Lorem ipsum dolor sit amet consectetur. Some marketing pitch going here.

Learn more about RFIs

Find the intelligence you need and get answers fast with Flashpoint Cyber Threat Intelligence. Flashpoint CTI delivers tailored and comprehensive intelligence across the deep, dark and surface web to help analysts focus on threats that matter, make smarter decisions and protect their people, places and assets.

With Cyber Threat Intelligence, you can:

- Protect against evolving threat actors groups, current events, malware families and ransomware crimes
- Understand active threats specific to your organization and industry
- Identify exposed assets, leaked credentials, and monitor threat actor conversations

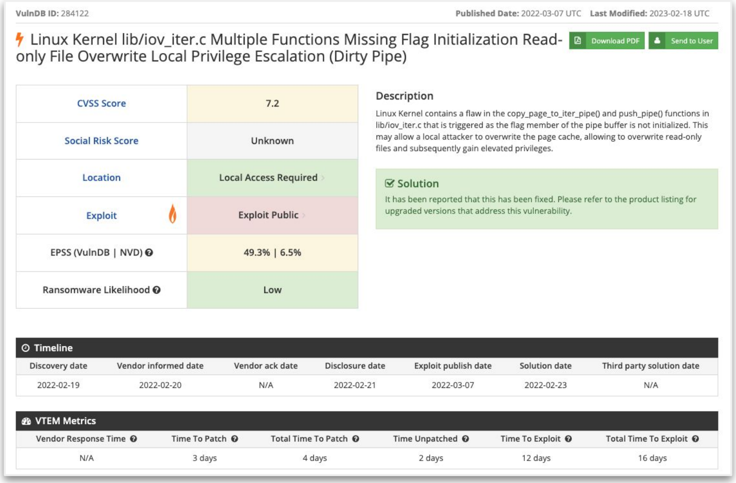
Vulnerability Management (VulnDB)

The most comprehensive and timely source of vulnerability intelligence and third-party library monitoring

Search for and be alerted on the latest vulnerabilities, both in end-user software and third-party libraries, for efficient prioritization and faster remediation of the vulnerabilities that matter.

With VulnDB, you can:

- Detect more vulnerabilities (including 97K+ without CVE ID) two weeks faster, on average, than CVE/NVD
- Prioritize and remediate based on 60+ fields of independently-researched advanced metadata
- Understand the likelihood that a vulnerability will be used in ransomware or actively exploited (EPSS) to better prioritize remediation efforts
- Leverage the SaaS platform or incorporate into existing workflows via API or integrations with commonly used tools like ServiceNow and Splunk



VulnDB ID: 284122 **Published Date:** 2022-03-07 UTC **Last Modified:** 2023-02-18 UTC

Linux Kernel lib/iov_iter.c Multiple Functions Missing Flag Initialization Read-only File Overwrite Local Privilege Escalation (Dirty Pipe)

CVSS Score	7.2
Social Risk Score	Unknown
Location	Local Access Required
Exploit	Exploit Public
EPSS (VulnDB | NVD)	49.3% | 6.5%
Ransomware Likelihood	Low

Description

Linux Kernel contains a flaw in the copy_page_to_iter_pipe() and push_pipe() functions in lib/iov_iter.c that is triggered as the flag member of the pipe buffer is not initialized. This may allow a local attacker to overwrite the page cache, allowing to overwrite read-only files and subsequently gain elevated privileges.

Solution

It has been reported that this has been fixed. Please refer to the product listing for upgraded versions that address this vulnerability.

Timeline

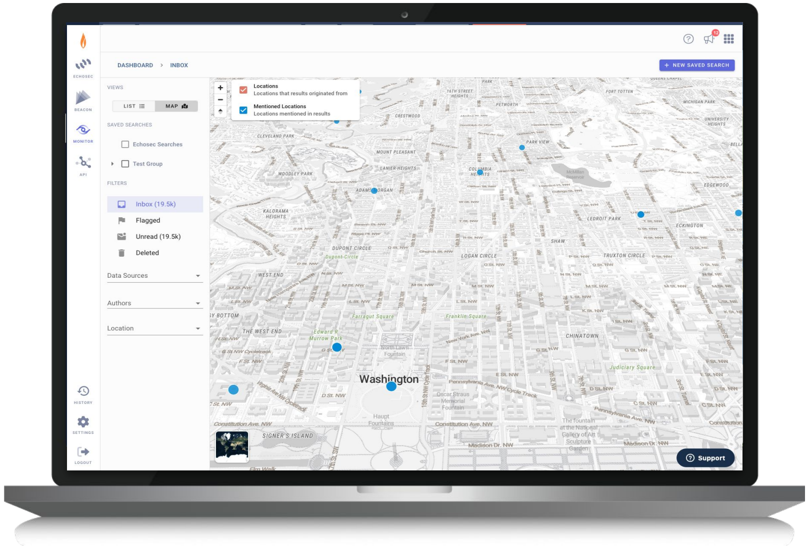
Discovery date	Vendor informed date	Vendor ack date	Disclosure date	Exploit publish date	Solution date	Third party solution date
2022-02-19	2022-02-20	N/A	2022-02-21	2022-03-07	2022-02-23	N/A

VTEM Metrics

Vendor Response Time	Time To Patch	Total Time To Patch	Time Unpatched	Time To Exploit	Total Time To Exploit
N/A	3 days	4 days	2 days	12 days	16 days

Physical Security Intelligence (formerly Echosec)

Real-time open-source intelligence and critical alerts to protect people, places, and assets



Protect the locations and assets that matter, get real-time alerts when critical events occur, and equip your team with the information and tools needed for proactive, intelligence-led physical security.

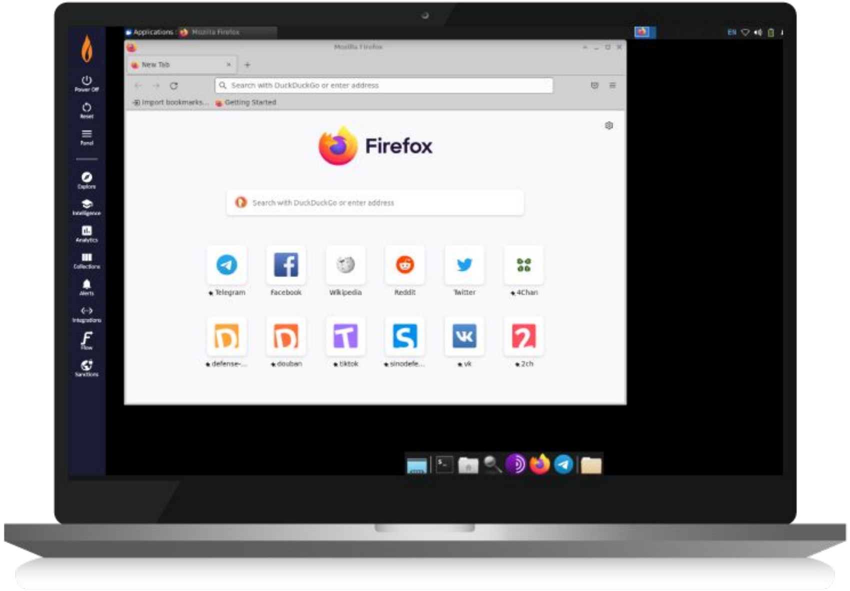
Physical Security Intelligence enables you to:

- Improve situational awareness with real-time data from social media and online discussions
- Accelerate investigations with geospatial AI, threat detection, and advanced search filters
- Protect executives, locations, and assets with 24/7 keyword and location monitoring
- Bolster your team with one-click access to our intelligence experts
- Identify relevant risks with custom alerts based on your search queries

Supporting Products

Managed Attribution

Directly investigate threats and reduce risk of exposure



Interact with files, conduct online investigations, and browse safely without risk to your organization. Managed Attribution is fully isolated from your browsers, computers, and network infrastructure to protect from malware and other malicious online threats.

With Managed Attribution you can:

- Protect your employees' computers and network
- Manipulate your digital fingerprint and configure your traffic to originate from anywhere in the world
- Take collections further and deepen your research capabilities

Automate

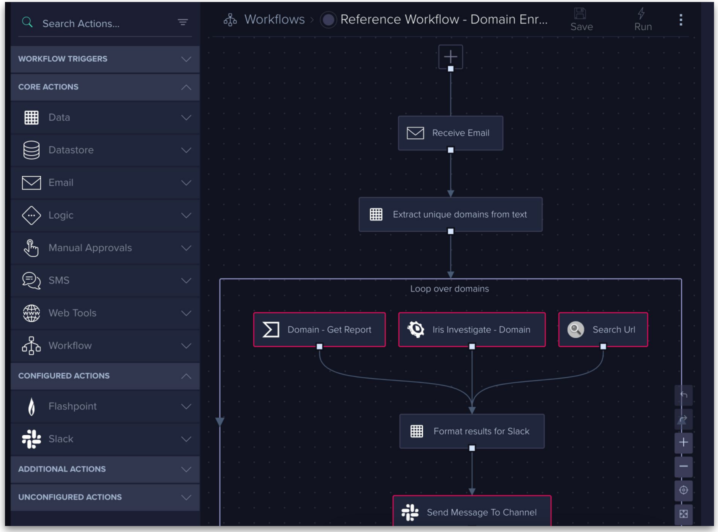
Protect your assets and eliminate manual work with automated workflows

Flashpoint Automate is the low-code automation platform integrated into Flashpoint solutions to accelerate repeatable security-related processes in order to help detect, analyze, and remediate risk faster.

With Flashpoint Automate, you can:

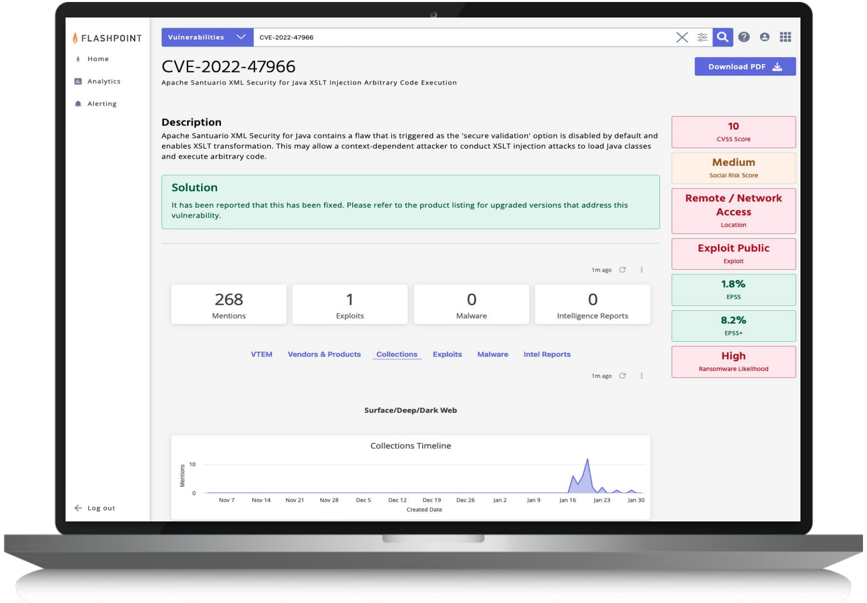
- Increase efficiency and save time with automated workflows
- Align resources to higher priority and complex investigations and response
- Take action based on better informed decisions

**Automate implementation services available upon request*



Vulnerability Intelligence for CTI Teams

World’s most powerful vulnerability dataset delivers a strategic view into vulnerabilities



CVE-2022-47966

CVE-2022-47966

Apache Santuario XML Security for Java XSLT Injection Arbitrary Code Execution

Description

Apache Santuario XML Security for Java contains a flaw that is triggered as the 'secure validation' option is disabled by default and enables XSLT transformation. This may allow a context-dependent attacker to conduct XSLT injection attacks to load Java classes and execute arbitrary code.

Solution

It has been reported that this has been fixed. Please refer to the product listing for upgraded versions that address this vulnerability.

268 Mentions	1 Exploits	0 Malware	0 Intelligence Reports

10 CVSS Score

Medium Social Risk Score

Remote / Network Access Location

Exploit Public Exploit

1.8% EPSS

8.2% EPSS+

High Ransomware Likelihood

Surface/Deep/Dark Web

Arm security teams across the organization with the intelligence and contextual information needed to effectively identify, prioritize and remediate vulnerabilities.

With Vulnerability Intelligence, you can:

- Gain a comprehensive view of vulnerabilities, including those mapped to malware, CVEs, and TTPs
- Search for closed and open source intelligence related to vulnerabilities (threat actor communications, message boards)
- Gain insights into vulnerabilities weeks before CVEs are available in NVD as well as 97K+ vulnerabilities not covered by CVE/NVD
- Leverage enriched data (EPSS, ransomware likelihood score, social risk score, temporal analysis) to help security teams prioritize vulnerabilities

Compromised Credential Monitoring

Proactively prevent fraud and account takeover originating from stolen credentials

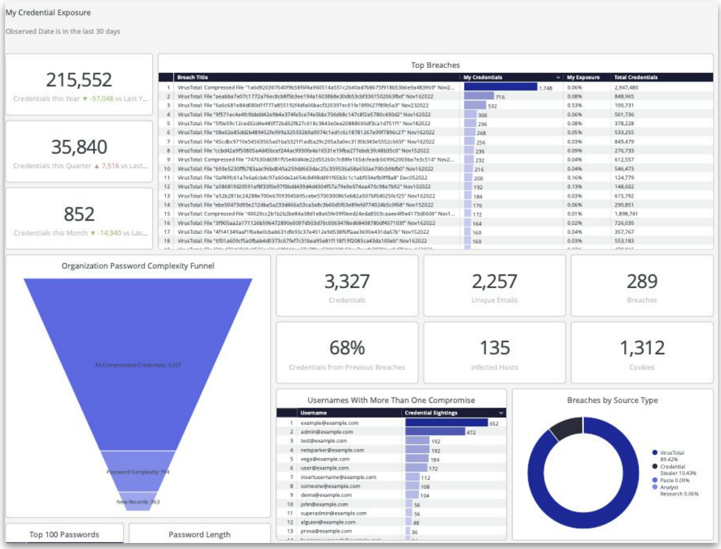
CCM- Enterprise

- Monitor stolen employee accounts for future sessions
- Identify employer-owned machines to take swift action
- Enforce strict password policy
- Prevent bypassing MFA
- Receive monthly exposure reports

CCM- Customer

- Monitor and flag stolen customer accounts for future sessions
- Remediate risks faster by quickly identifying client accounts that have been compromised
- Leverage customer password data to identify risk, reset customer password, improve your security posture, and prevent fraud loss

**CCM implementation services available upon request*



My Credential Exposure

Observed Date is in the last 30 days

215,552
Credentials this Year ▼ -57,048 vs Last Y...

35,840
Credentials this Quarter ▲ 7,516 vs Last...

852
Credentials this Month ▼ -14,940 vs Las...

Top Breaches

	Breach Title	My Credentials	My Exposure	Total Credentials
1	VirusTotal: Compressed File "1a6d920307640f9b58f6f4a960514a551c2640ad7b8675f918b53b6e9a483969" Nov2...	1,748	0.06%	2,947,480
2	VirusTotal: File "aeabba7e07c1772a76ec8cb8f5b3ee194a16038b8e30db53cbf3361502063fbd" Nov162022	716	0.08%	848,965
3	VirusTotal: File "6a6c681e84d080d1f777a855192f4dfa06bacf320397ec01fa18f0627f89b5a3" Nov232022	532	0.53%	100,731
4	VirusTotal: File "9f571ec4e4fc9bbdd42e9b4e374fe5ce74e5bbc706d68c147c8f2e5780c430d2" Nov162022	300	0.06%	501,736
5	VirusTotal: File "5f0e59c12ced32d4e480f72bd32f827c618c3843e0ee20888600df3ca1d751f1" Nov182022	296	0.08%	378,228
6	VirusTotal: File "08e02e85dd2b489452fe999a325932b9a9074c1ed1c6c18781267e99f7896c27" Nov162022	268	0.05%	533,255
7	VirusTotal: File "45cdbc9710e54563565ad1ba5321f1ad5a29c205a3a0ec3130b343e5552c665f" Nov162022	256	0.03%	849,479
8	VirusTotal: File "ccbd42a9f50805a4d45bcef244ac9930fa4a16531e19fba277ebdc3fc48b35c0" Nov152022	236	0.09%	276,733
9	VirusTotal: Compressed File "747630dd381f55e40d4de22d55260c7c88fe165dcfeadc669962003ba7e3c514" Nov2...	232	0.04%	612,557
10	VirusTotal: File "b93e5230ffb783aac96bd045a259dd663dac25c359536a58a650ae700cb9bfb0" Nov162022	216	0.04%	546,473
11	VirusTotal: File "0af49fc61a7e6a6cb4c97a60de2a654c8498dd91f65b3c1c1abf034efb9ff8a8" Dec052022	200	0.16%	124,779
12	VirusTotal: File "a58681fd20591ef8f33f0e97f0bdd439d4d4304f57a79e9e074aa470c98e7b92" Nov102022	192	0.13%	148,602
13	VirusTotal: File "a52b281bc24288e700e67093945b95cebe5700300865eb82a507bf0d0250cf25" Nov162022	184	0.03%	615,792
14	VirusTotal: File "ebe50473d93e2124ba5a233d466a53ca3a8c3b60d5f63e89efd774024b5c0f68" Nov152022	176	0.06%	290,851
15	VirusTotal: Compressed File "40620cc2b1b2b2be84a38d1e8a65fe09f0eed24eda8503caaee4f0e4173d0600" Nov1...	172	0.01%	1,898,741
16	VirusTotal: File "3f905aa2a171126b596472890e0097d503d70c0063478ed68408780df457103f" Nov162022	164	0.02%	726,035
17	VirusTotal: File "4f141349aaf1f6ebe0cbab631dfe93c37e4512e9d538f6ffaae3690e431da67b" Nov152022	160	0.04%	357,767
18	VirusTotal: File "6f01a609cf5a0fbab4d0373c67fef7c31bea95e81f118f19f2085ca43da100eb" Nov162022	160	0.03%	553,183

Organization Password Complexity Funnel

3,327
Credentials

2,257
Unique Emails

289
Breaches

68%
Credentials from Previous Breaches

135
Infected Hosts

1,312
Cookies

Usernames With More Than One Compromise

	Username	Credential Sightings
1	example@example.com	652
2	admin@example.com	472
3	test@example.com	192
4	netsparker@example.com	192
5	vega@example.com	184
6	user@example.com	172
7	insertusername@example.com	112
8	someone@example.com	108
9	demo@example.com	104
10	john@example.com	56
11	superadmin@example.com	56
12	alguien@example.com	48
13	prova@example.com	36

Breaches by Source Type

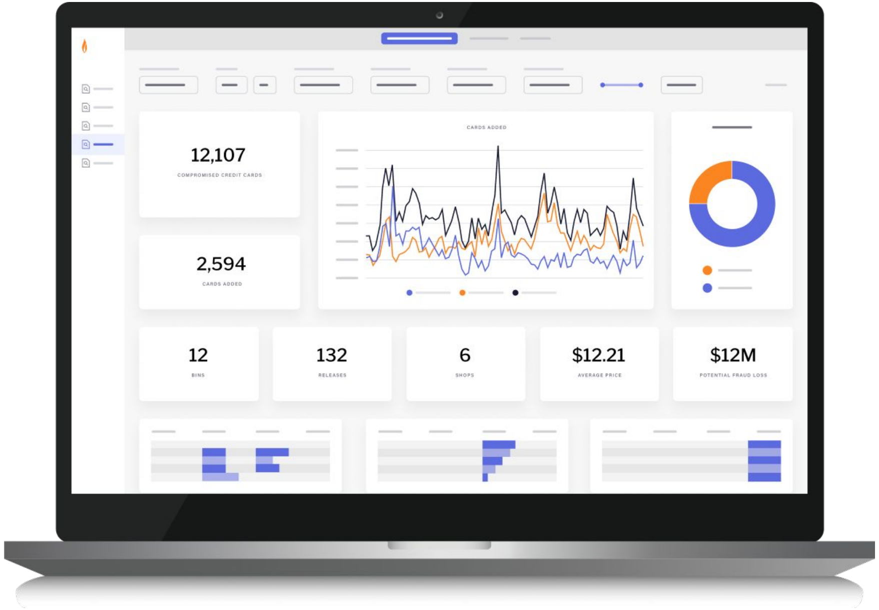
Top 100 Passwords

Password Length

CCM-E "My Credential Exposure" Dashboard

Card Fraud Mitigation

Financial intelligence throughout the lifecycle of a stolen credit card



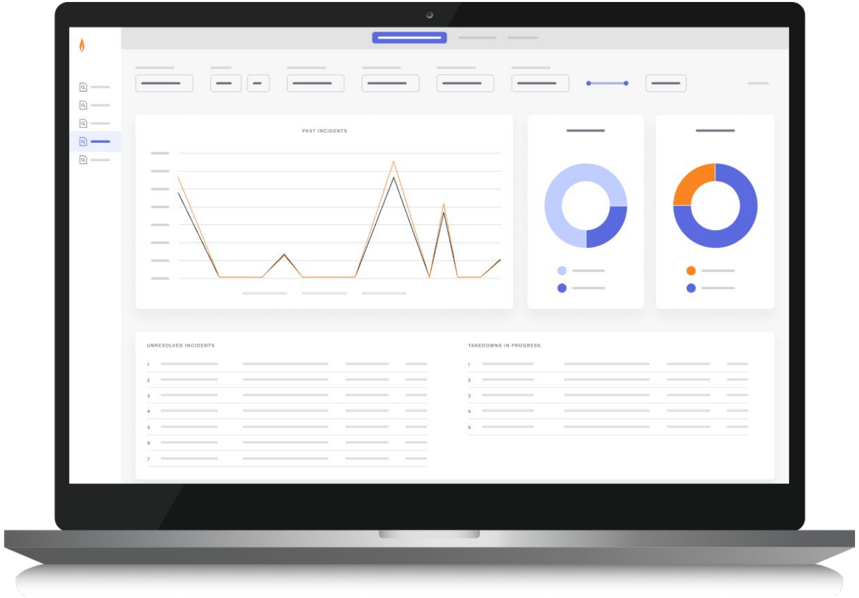
Detect compromised credit cards from illicit communities and data breaches, and identify high-risk merchants before fraudulent transactions occur to prevent monetary loss and reduce reputational risk.

With Card Fraud Mitigation, you can:

- Make faster, more confident decisions
- Bolster collaboration between departments
- Free up your time and focus on more impactful work

Brand Exposure Protection

Protect your brand, reputation and customers from external threats



Prioritize and take action to remediate malicious URLs, fake social media accounts, fraudulent mobile apps and more.

With Brand Exposure Protection, you can:

- Monitor for brand impersonations
- Stop typosquatting
- Request takedowns

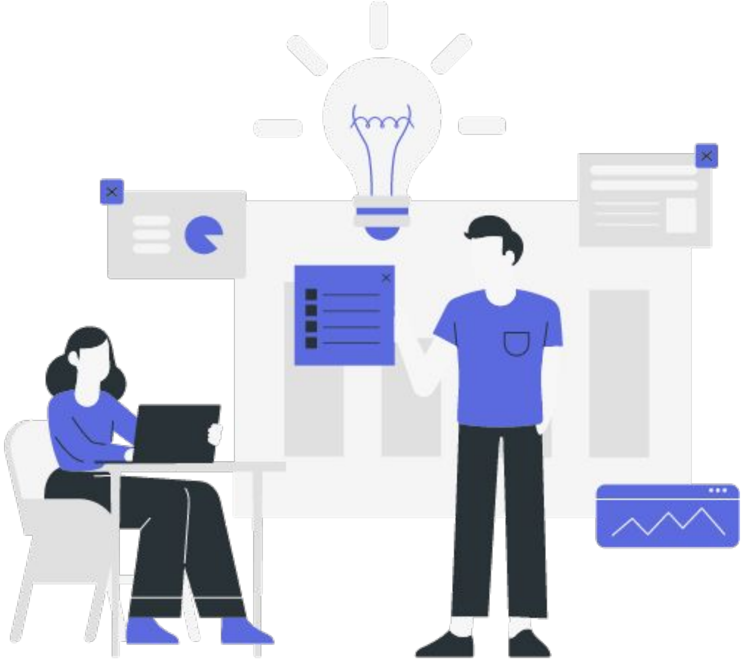
Services

Services Overview

Flashpoint helps reduce the challenges faced by overwhelmed or under-resourced intelligence and security functions, and can accelerate growth in both capability and efficiency for new or expanding teams.

Flashpoint offers the following service types:

- Managed Intelligence Services - sustained or on-demand
- Professional Services - on or offsite
- Implementation - available for specific products



Managed Intelligence Services

Scale your operations to combat and mitigate threats to your organization.

Curated Alerting

Get relevant tactical analysis and risk assessments from illicit online communities, based on continual monitoring of intelligence requirements (IRs). Flashpoint works with customers to create optimal queries, capturing customer-prioritized keywords and identifiers.

With Curated Alerting, you can:

- Receive analyst-crafted assessments based on content collected from Flashpoint collections
- Leverage Flashpoint analysts to help formulate alert keywords that pertain specifically to your intelligence requirements
- Save time reviewing large quantities of results by allowing Flashpoint analysts to use their expertise and understanding of online communities to highlight the noteworthy items
- Request proactive acquisition of advertised items like logs, accesses, tutorials, and hijacked accounts based on your standing intelligence requirements (**Proactive Acquisitions**)

Request for Information

Through the RFI process, Flashpoint intelligence analysts field questions and conduct research inside closed illicit online communities and open sources to provide original, unique analysis and help your team fill intelligence gaps.

With the Request for Information service, you can:.

- Address intelligence requirements through tailored analysis by submitting requests directly to Flashpoint analysts
- Gain unique insights with innovative technology and collections processing
- Leverage industry-leading intelligence experts to rapidly analyze, refine, and contextualize data to produce valuable insights

Tailored Reporting Service

Flashpoint's Tailored Reporting Service (TRS) provides a tailored weekly or monthly deliverable that addresses specific intelligence requirements and highlights relevant threats with further assessments—saving analyst time and equipping teams with the resources to stay informed of the organization's threat landscape.

With Tailored Reporting, you can:

- Receive tactical and operational intelligence on key threats
- Develop greater depth and context with strategic, human-readable reporting to tactical, programmatic feeds
- Receive relevant threat actor tactics, techniques, and procedures (TTPs), campaigns, and context that transforms data into intelligence
- Build a stronger bench of resources and collections

Analyst Support

Flashpoint provides various types of analyst support based on your unique requirements.

Staff augmentation:

Force multiply your team with onsite or virtual staff providing full-time intelligence analyst support.

Sustained support:

Take a proactive approach by employing Flashpoint to produce in-depth intelligence assessments to rapidly identify threats and mitigate your most critical security risks.

Collection Discovery

Leverage Flashpoint analysts to identify new illicit communities to collect for inclusion into the Flashpoint platform to enable workflows and reporting. Includes two proactive searches per week.

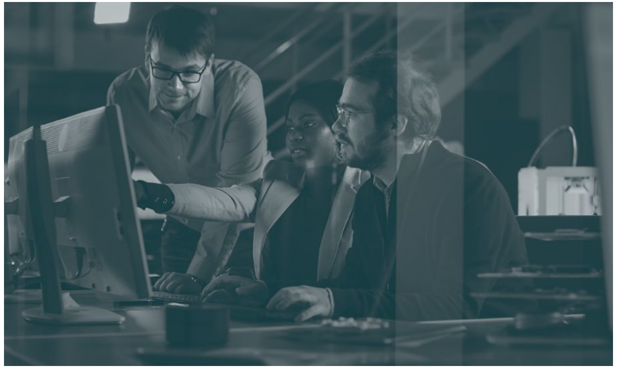
Professional Services

Reduce time to decision making and gain the advantage in combating threats and mitigating risk.

Threat Response and Readiness

Ransomware and extortion are responsible for billions of dollars in losses each year across industries. While some high-profile attacks and success stories reach the mainstream, they are a tiny percentage of the true number of incidents and actual payouts made to adversaries.

When an organization is targeted by ransomware or cyber extortion, it must quickly determine the extent of the attack, determine the response plan, and mitigate the impact.

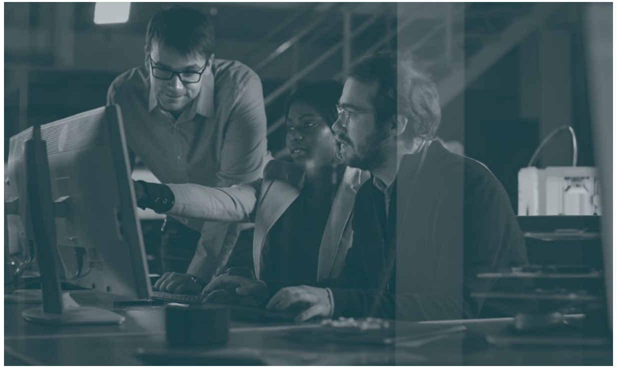


With Flashpoint's Threat Response and Readiness service, we help you:

- Evaluate and test for ransomware or cyber extortion event preparedness
- Assess and respond to a ransomware or cyber extortion attack
- Determine the credibility of attacker claims
- Engage safely in negotiation and transactions
- Return quickly to business continuity

Threat Actor Engagement & Procurement

With Threat Actor Engagement & Procurement, Flashpoint anonymously and securely engages with a specific threat actor on behalf of your organization.



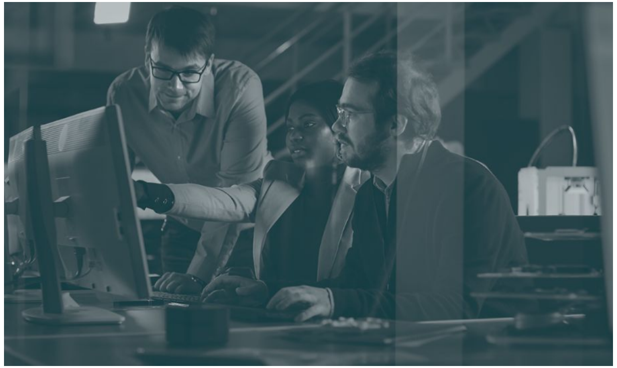
Service may include:

- Coordinate a threat actor engagement to identify the possible source of the material or data
- Validate the sources and information
- Purchase or otherwise obtain the specific data and arrange for any other communications with the actors

This is not an ongoing service but is meant to be used in response to a particular incident.

Extortion Monitoring

In the case of a breach, stolen data could end up on illicit markets months or years after the initial compromise has occurred. Flashpoint supports investigative efforts, response, and recovery.

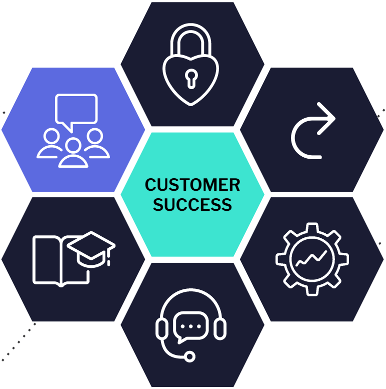


Extortion Monitoring provides pre-and post-event monitoring of keywords in Flashpoint holdings based on your requirements, critical for continuous assessment of reputation and legal obligations beyond the conclusion of an investigation or incident response.

Customer Success, Partners, & Integrations

Flashpoint Customer Success

Working in concert with our customers to accelerate adoption and maximize outcome attainment



Customer Engagement

- Adoption Enablement : Product and Intelligence Support
- Proactive Outreach/Support: Recurring Touchpoints
- Outcome Realization

Customer

- Product Feedback
- Ongoing Success Criteria
- Successes/Challenges

Professional Services

- Implementation Support
- Advisory Services
- Tailored Training / Staff Augmentation

Onboarding

- Platform training and case studies
- Facilitate time to initial value
- Initial product tuning/time-to-value

Education Services

- On-demand and live solution training
- Value Acceleration
- Curated Content Creation

Customer Support

- Troubleshooting
- How To
- Crisis Management

- Collectively over 120 years of intelligence professional experience
- US Government and Military intelligence experience
- Private sector cybersecurity intelligence experience across industries
- Dedicated team supporting Flashpoint National Security Solutions customers

Who we partner with

Flashpoint provides thoughtful support to SPARK Partner Alliance members that market, sell, and deliver our suite of converged intelligence and risk solutions to public and private-sector organizations around the world

Business Consultants and Advisory Firms

As trusted advisors to your clients, we help grow your toolkit to identify the comprehensive solutions to tough global challenges.

Value-Added Resellers (VARs)

Flashpoints suite of products and services help expand your offerings to provide your clients with more robust services that meet their expanding needs.

Managed Security Service Providers (MSSPs)

Flashpoint works with your company to extend the capabilities of your branded cybersecurity and threat response solutions.

Systems Integrators and OEMs

With Flashpoints array of API endpoints designed to empower users with the context they need to make better decisions about cyber security, fraud, inside threats , and physical threats we can help you take a richer product mix to market that can be customized to the needs of any customer worldwide.

Distributors

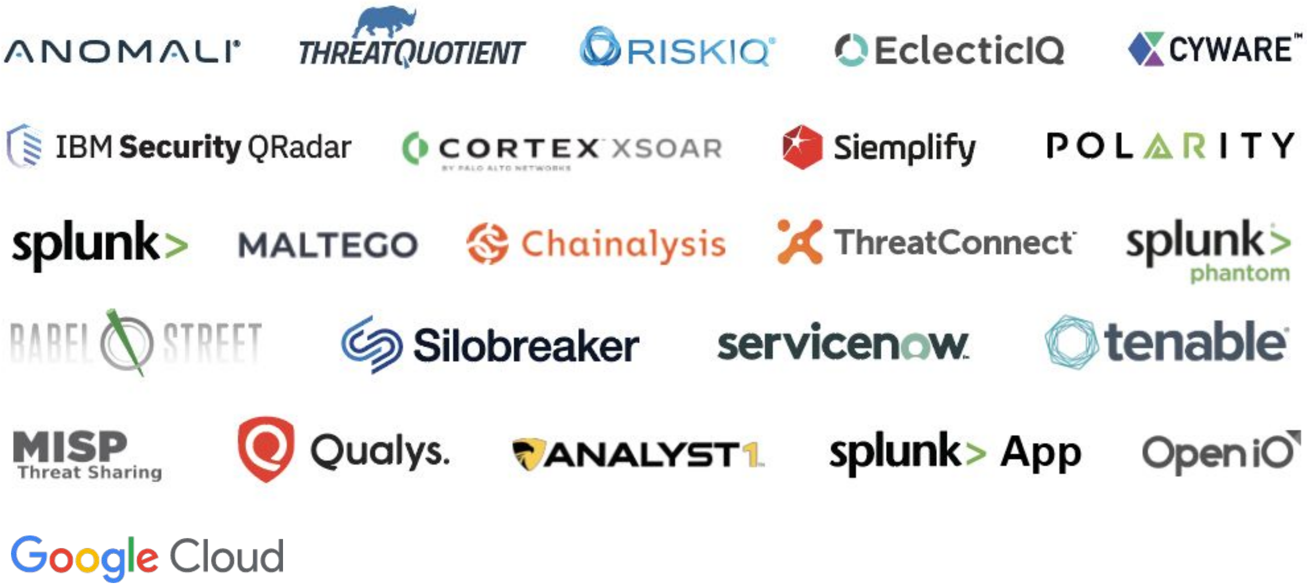
Maximize your portfolio of brands and deliver unique value to your network of vendor and clients.

Technology Partners

Flashpoint works with leading cybersecurity technology platforms to integrate additional data streams that bolster their intelligence mix and more robustly serve new customers.

Integration Partner Network

Our partners work with us to provide unmatched visibility into threats, empowering users with the context they need to make better decisions about cyber threats, fraud, and physical and insider threats.



FLASHPOINT

Thank you

flashpoint.io