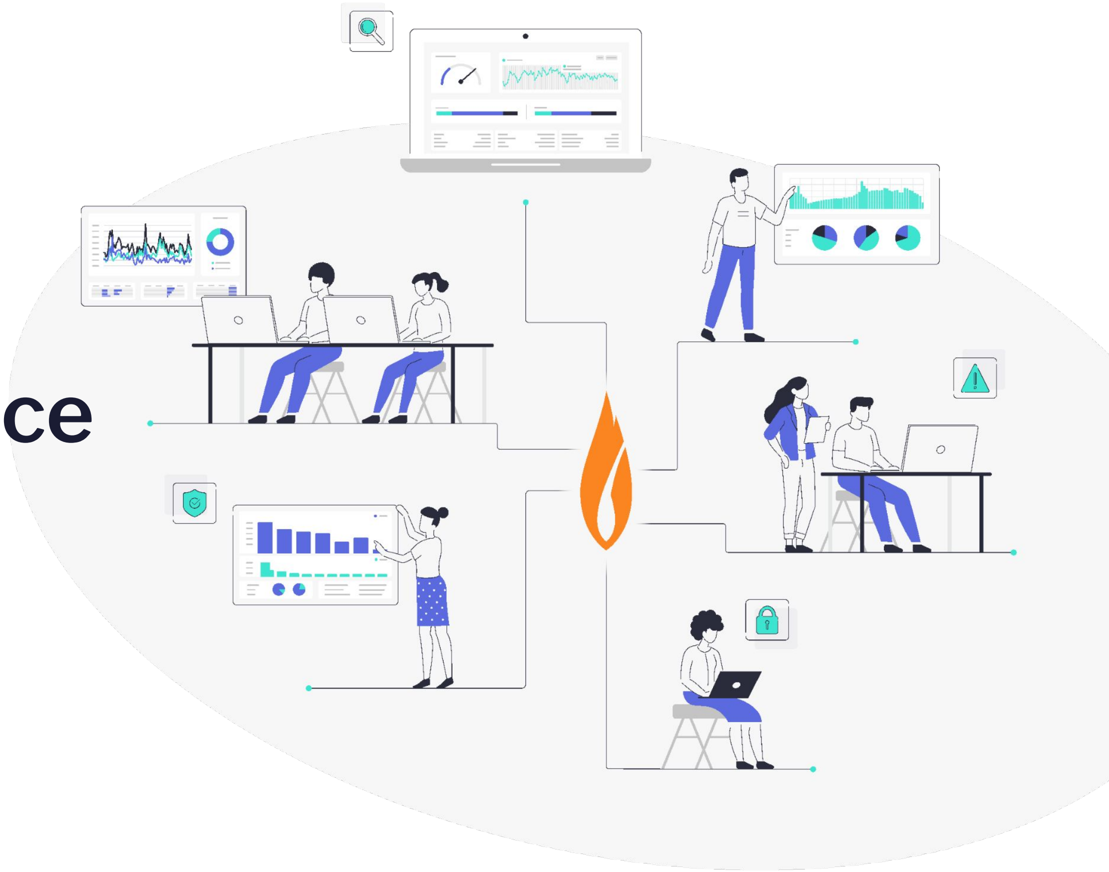
FLASHPOINT

Actionable and trusted intelligence for every team



Brendan Phelps
Senior Account Executive
bphelps@flashpoint.io

Agenda

- Open-Source Intelligence (OSINT) and its growing importance for organizations
- Who is Flashpoint and what do we do?
- Risk intelligence by sector
- Case study discussion: how we helped detect and prevent an attack on a Jewish synagogue in NYC
- Questions and answers

Search by location...

biden "saudi arabia"

OPEC+ seen considering deeper supply cuts as market falters | The Edge Markets

- A + A (Nov 29): OPEC and its allies are expected to consider deeper supply curbs when they meet this weekend against the backdrop of a faltering global oil market. Saudi Arabia and its partners surprised ers — and drew a fierce rebuke from

Monday, November 28, 2022 17:42

JoJoFromJerz

HOLY SHIT. Shell has reported profits of $9.5 billion for the third quarter compared to $4.1 billion in the same quarter last year.

But tell me more about how high gas prices are Joe Biden's fault, won't you.

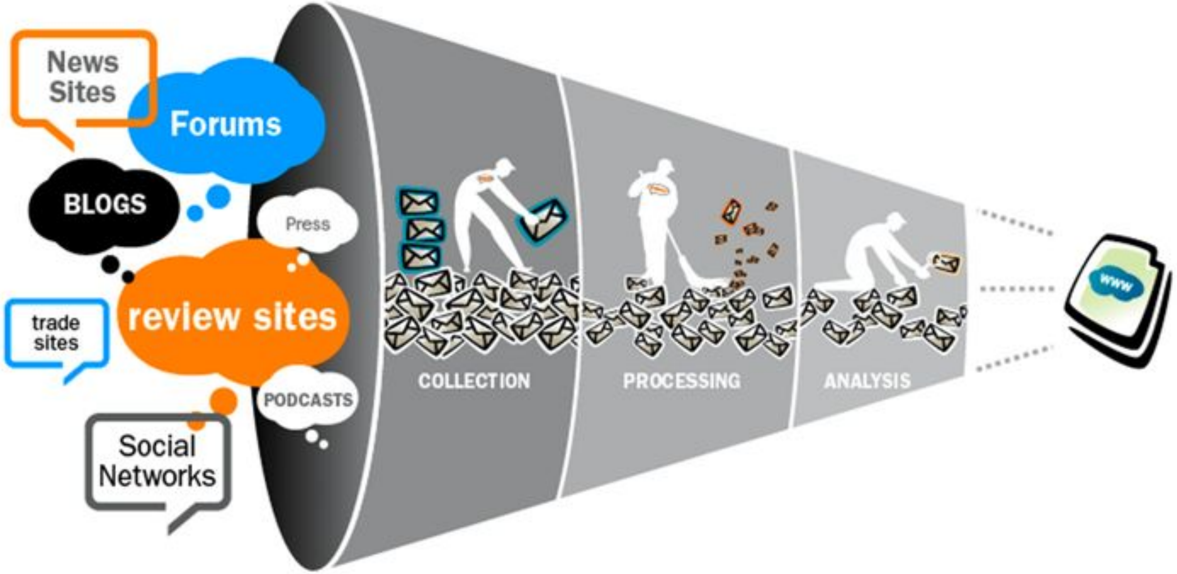
FFS.

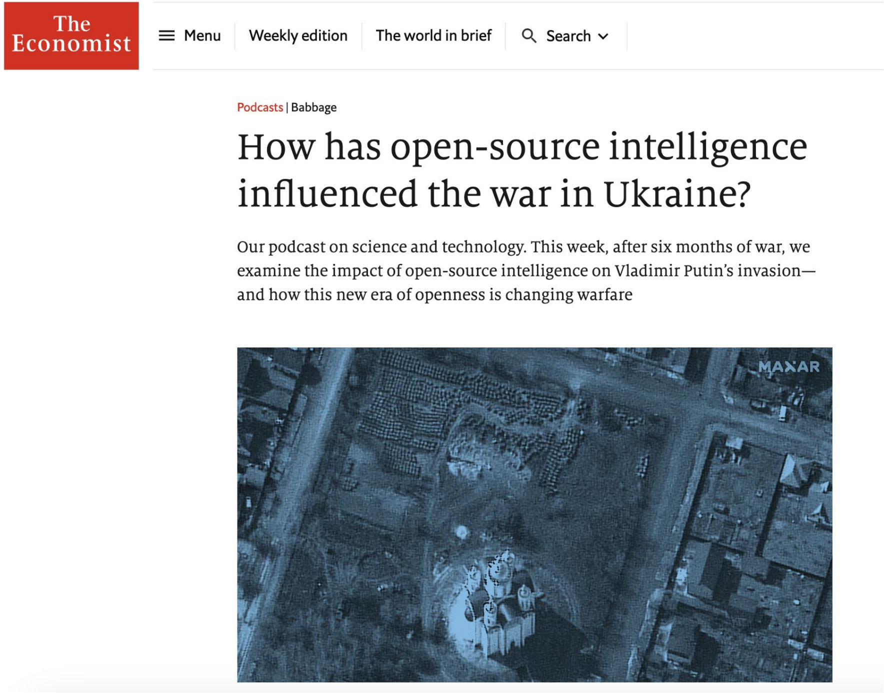
9:17 AM · 10/27/22 · Twitter for iPhone

able efforts are made to ensure that fuel pri cation are accurate, fuel prices are s guaranteed offer.

What is Open-Source Intelligence (OSINT)?

The collection and analysis of data gathered from public sources to produce actionable intelligence

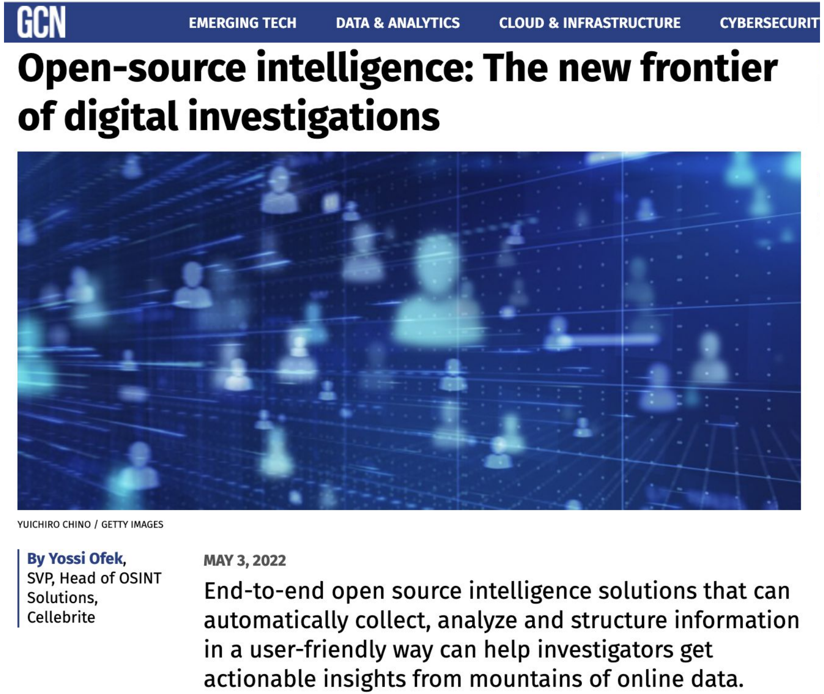




Podcasts | Babbage

How has open-source intelligence influenced the war in Ukraine?

Our podcast on science and technology. This week, after six months of war, we examine the impact of open-source intelligence on Vladimir Putin's invasion—and how this new era of openness is changing warfare



Open-source intelligence: The new frontier of digital investigations

YUICHIRO CHINO / GETTY IMAGES

By Yossi Ofek,
SVP, Head of OSINT Solutions, Cellebrite

MAY 3, 2022

End-to-end open source intelligence solutions that can automatically collect, analyze and structure information in a user-friendly way can help investigators get actionable insights from mountains of online data.

Who is Flashpoint?

Flashpoint is an intelligence company, helping organizations **close the gap between data, intelligence, and action**, to detect and mitigate digital and physical risks

700+
Clients

50+
Countries

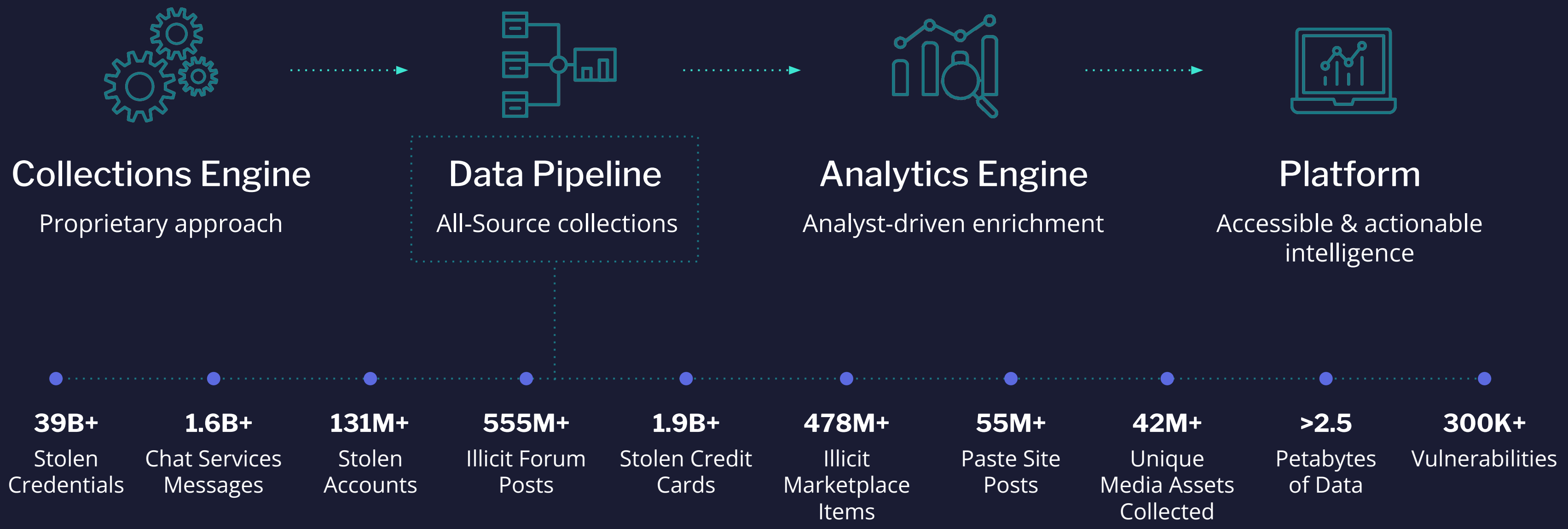
30+
Industries

Intelligence analyst expertise

100+ experts who speak 35+ languages

Deep intel and security expertise across military, government and Fortune 500s

Best-in-class intelligence and advanced analytic tradecraft



Collections Engine

Proprietary approach

Data Pipeline

All-Source collections

Analytics Engine

Analyst-driven enrichment

Platform

Accessible & actionable intelligence

39B+ Stolen Credentials

1.6B+ Chat Services Messages

131M+ Stolen Accounts

555M+ Illicit Forum Posts

1.9B+ Stolen Credit Cards

478M+ Illicit Marketplace Items

55M+ Paste Site Posts

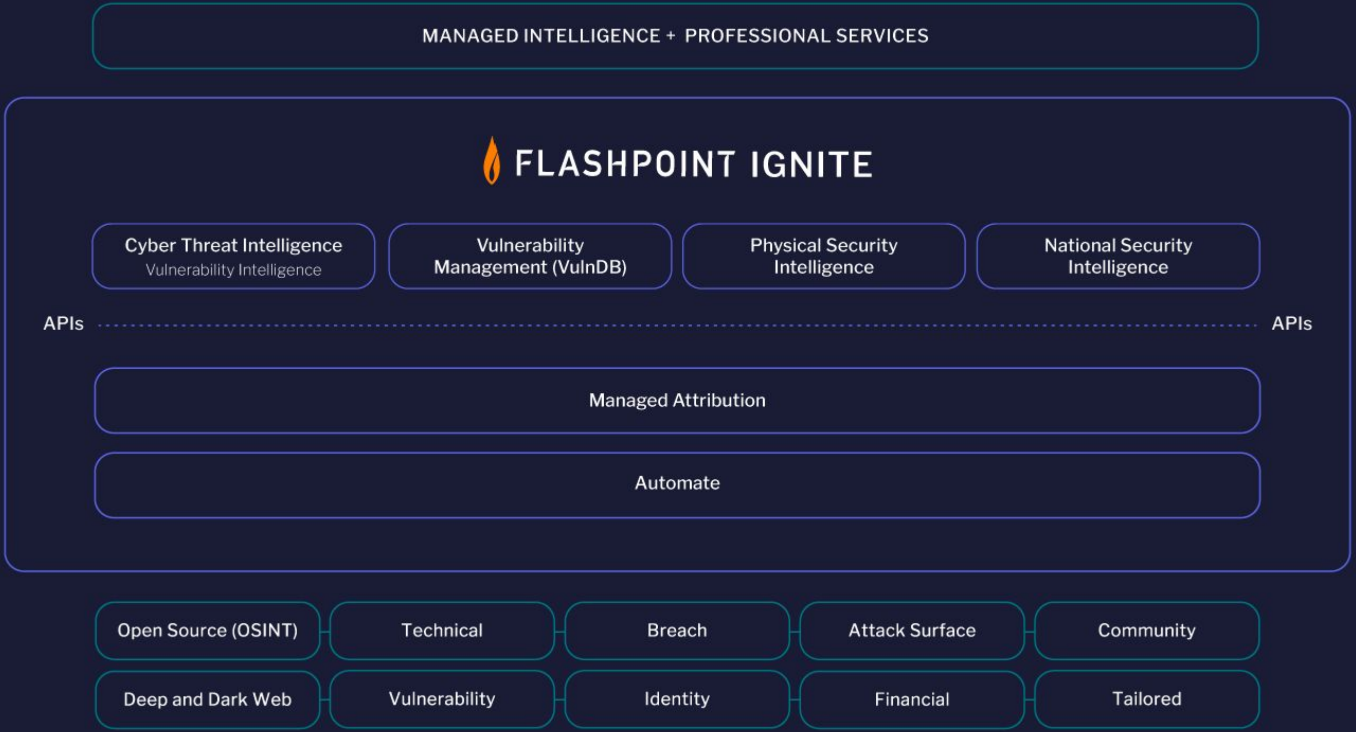
42M+ Unique Media Assets Collected

>2.5 Petabytes of Data

300K+ Vulnerabilities

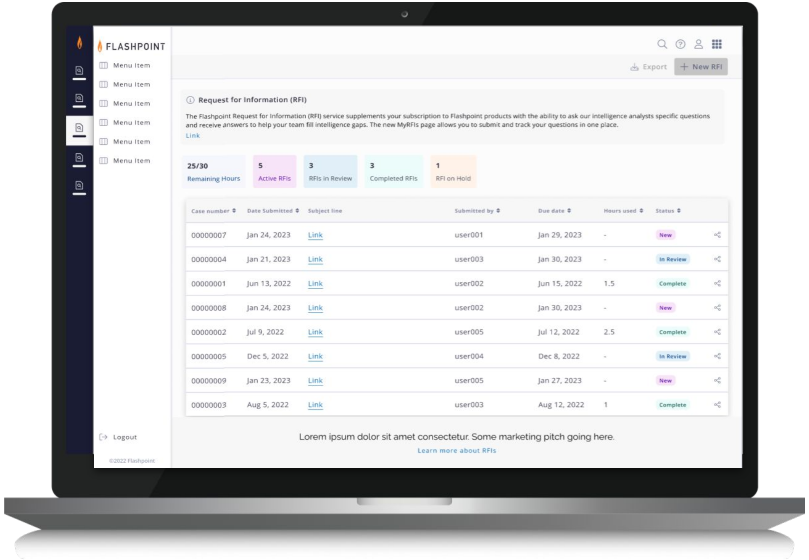
Flashpoint Ignite Platform

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

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

Private Sector Risk Intelligence

(Financial, Retail, Healthcare, Technology, etc.)

Financial fraud - access illicit online communities to detect compromised bank accounts and credit cards for sale, and detect phishing pages seeking to steal customer's personal information

Retail fraud - understand the tactics, techniques and procedures threat actors are using to defraud your company (ie. gift card fraud, account takeovers, or refund fraud like empty box/wrong item/did not arrive methods)

Executive protection - monitor mentions of public facing executives (ie. CEO) for violent posts that might indicate a threat to their safety

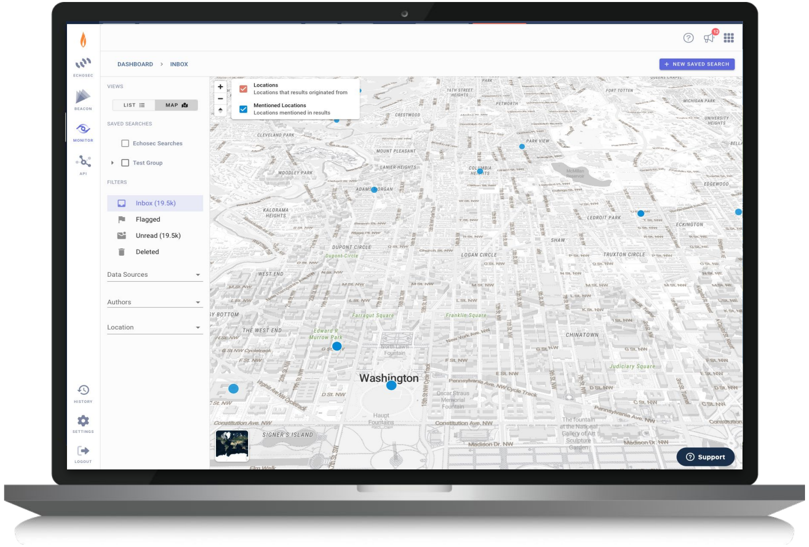
Property protection - detect potential threats against physical locations like offices, facilities, stores and event venues

Ransomware response - track emerging ransomware campaigns and have a cyber extortion plan in place to mitigate the financial impact

Insider threats - uncover insider threats in hidden online communities where intellectual property is bought and sold

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
- Identify relevant risks with custom alerts based on your search queries

Public Sector Risk Intelligence

(Military, Government, Law Enforcement, etc.)

Geopolitical risk assessment - track areas with evolving political unrest to understand developments in the region (ie. Ukraine)

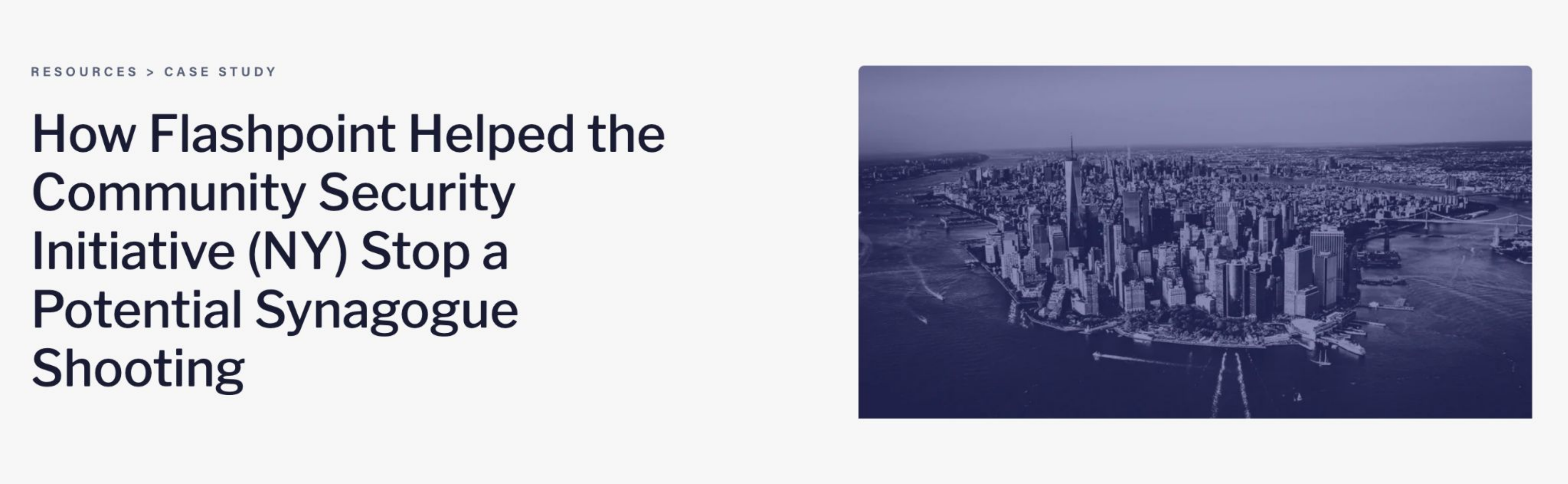
Force protection - monitor active hostile war zones for imminent threats to personnel on-the-ground (ie. Kabul)

Counterterrorism - gain insight into criminal terrorist organizations, how and where they operate online, communicate with each other, recruit new members, and spread propaganda (ie. Islamic State)

Crisis response - respond to threats to public safety (ie. active shooters, natural disasters, etc.)

Disinformation monitoring - monitor misinformation and disinformation online to track issues that could escalate to real-word security events (ie. Stop the Steal / Capitol riots, COVID-19 / Freedom Convoy)

Case Study



RESOURCES > CASE STUDY

How Flashpoint Helped the Community Security Initiative (NY) Stop a Potential Synagogue Shooting

https://flashpoint.io/resources/case-study/how-flashpoint-helped-csi-stop-potential-synagogue-shooting/

Background

- New York City is home to approximately 1.6 million Jewish people and 2,400 Jewish institutions

- The Community Security Initiative, made up of the United Jewish Appeal Federation and the Jewish Community Relations Council, is responsible for protecting the Jewish population in New York City, Long Island and Westchester

- Led by the former director of intelligence for the NYPD, the Community Security Initiative is a 12-person team that monitors the online threat landscape and sends alerts to members of the Jewish community

- Following a rise in antisemitism, threats of violence, and deadly attacks at Jewish synagogues in the US, the Community Security Initiative needed a way to filter the online chatter, specifically on social media, to detect real threats

COMMUNITY SECURITY INITIATIVE

A JOINT PROGRAM OF

Jewish Federation & Foundation OF ROCKLAND COUNTY

UJA Federation NEW YORK

JCRC JEWISH COMMUNITY RELATIONS COUNCIL OF NEW YORK UNITING COMMUNITIES

Our Role

- The Community Security Initiative needed an effective tool to monitor and filter mainstream and niche social media networks
- They were already monitoring the deep/dark web with Flashpoint, and Echosec had just been acquired, so we connected with the team to set up a trial of the platform
- We helped their team set up location and keyword searches with advanced filters to detect mentions of social media posts that might indicate a threat
- Within the first 4 weeks, the team was alerted to a concerning social media post on Twitter that prompted them to investigate the user in question

Timeline

- Friday, November 18, 2022, 10:30am - Community Security Initiative team gets alerted to two Tweets by the same user:
    - “Big moves being made on Friday”
    - “Gonna ask a Priest if I should become a husband or shoot up a synagogue and die”
- Another post by the same user (“This time I’m really gonna do it”) reinforced the threat, indicated the attack could be carried out after 10:00pm Friday night with a willingness to “die by cop.”
- A quick username search uncovered other online profiles using the same @handle with more threatening content
- Community Security Initiative team notified law enforcement in New York City and Long Island, which led to a coordinated manhunt with the NYPD and FBI

Outcome

- Just before midnight, two officers spotted the man at Penn Station with another man
- Both suspects were arrested on charges of conspiracy and weapons possession
- At the time of the arrest, authorities seized a Glock 17 with 30 rounds of ammunition, a bulletproof vest, military knife, ski mask and swastika armband
- One suspect admitted to operating a white supremacist group on social media and was also indicted on felony terrorism and hate crime charges

Outcome

ANTI-SEMITIC THREATS
PIX11
7:18
38°
lewark 35° Hi: 45 lo: 30°
Union City 37° Hi: 50 lo: 34°
Jersey City 37° Hi: 50 lo: 35

FLASHPOINT

Brendan Phelps
bphelps@flashpoint.io
1-250-415-6440