FLASHPOINT

Protecting Executives and Key Personnel With Social Media Intelligence

Executive Threats Are Diversifying

12x

Likelihood of the C-suite being targeted in a cyber attack[1]

$12 Billion

Total cost of executive impersonation scams (BEC)[2]

As a security professional, you probably know that executive threats now come from all directions: from unforeseen physical risks to doxing and negative press. Public online content, such as social media or illicit forums, is often the earliest and most accurate source of information for executive protection when it comes to digital security, physical security, and their intersection.

But without easy access to relevant threat indicators, security teams risk information gaps that can leave key personnel and their families vulnerable to data disclosure and physical harm.

Alongside traditional executive protection tools and strategies—like bodyguards and security cameras—specialized open-source intelligence (OSINT) software is crucial for surfacing this information and reducing blind spots. Flashpoint Physical Security Intelligence (PSI) provides users with an intuitive, comprehensive solution for detecting executive threats across across global social media, messaging apps, and illicit forums.

How has Flashpoint PSI supported executive protection professionals in real-world use cases?

1 Verizon: "2019 Data Breach Investigations Report," P. 3.
2 Federal Bureau of Investigation: "Business E-mail Compromise The 12 Billion Dollar Scam," Public Service Announcement, July 12, 2018: https://www.ic3.gov/Media/Y2018/PSA180712.

Case 1:
Online Extremism

Challenge:

A public sector security team wanted to keep tabs on online threats from extremist groups targeting high-profile public servants. In the wake of COVID-19 demonstrations and the Capitol Hill insurrection in January 2021, the team was concerned with proactively identifying physical threat indicators on more obscure, hard-to-access networks frequented by adversaries.

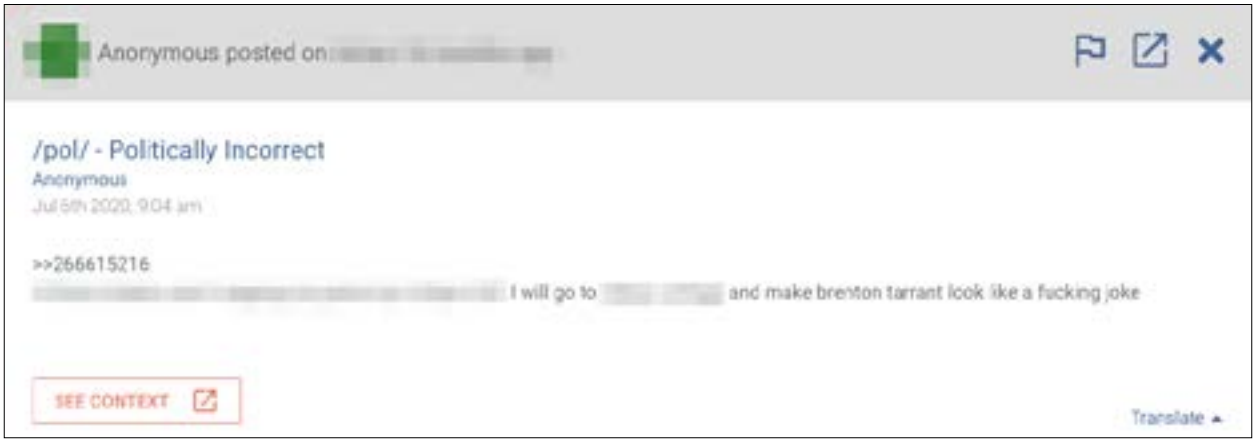
Process:

Flashpoint PSI crawls a wide range of deep web and dark web chan boards, forums, and alt-tech networks known to be used by domestic extremist groups. We identified a number of targeted threats to a Person of interest, including violent threats masked by coded language and references to perpetrators of mass shootings.

The security team's primary concern was to find early warning indicators originating from fringe online networks and extremist groups. However, Flashpoint's mainstream social network coverage and location-based searches provided additional functionality: the team could also use the tool to identify on-the-ground risks being documented by social media users in real-time.

Outcome:

Using Flashpoint PSI, these security professionals could now continuously monitor emerging networks for new threats to vulnerable individuals. They could also better predict on-the-ground activities like planned demonstrations and respond appropriately. Alongside their physical security detail, the team is better equipped to predict and respond to threats and keep public servants and their families safer.



Case 2:
Doxing and Data Breaches

Challenge:

Doxing is the act of leaking personally identifiable information (PII) on the web to maliciously target an individual, often as a form of retribution. A national law enforcement unit was looking for online threats targeting public officials in a North American city. They needed a specialized online search tool to safely monitor paste sites and deep and dark web spaces where explicit threats and doxing are common.

Process:

Flashpoint analysts used a Boolean search string combining a relevant location with some public official title keywords. The search returned dozens of results within seconds. One search result included a dox targeting one of the officials on a dark web discussion forum, including their contact information, home address, and a call to kill them and their family.

After finding this post, the search query was adjusted to focus specifically on the doxing victim. Additional doxes, including personal and family member information and incitement to target other public officials and their families were discovered.

Outcome:

In the short term, this discovery provided the unit with the information required to protect vulnerable personnel and their families from immediate harm. In the long term, the unit is now equipped with a solution to monitor its executive's personally identifiable information so that future risk indicators are flagged in near real-time and harm is minimized or avoided.

Case 3:
Travel Risk Management

Challenge:

In 2016, a security team required a threat intelligence platform to ensure VIP safety during the 2016 Rio Olympics. The team needed to monitor public social media content originating near the individual's travel routes and respond proactively to risks. For the security team, manually navigating social content was too slow for an efficient response—and competing search tools could not provide the data fidelity required for locating needle-in-the-haystack threat indicators.

Process:

Flashpoint PSI enabled the team to set up saved searches and monitor social networks for threats in real-time. The Platform's geofencing capability allowed them to monitor specific neighborhoods and travel routes within Rio for relevant content. Advanced filters also separated posts containing risk indicators like local disruptions, shootings, and other incidents that could validate a security response.

Outcome:

At a critical moment, Flashpoint notified the security team of a gun within one of its geofences. The alert was escalated and the team quickly rerouted the VIP to a secondary exit airport for a safe departure. Without Flashpoint PSI, the VIP could have encountered a potentially dangerous situation and risked injury. Now, the security team is equipped to handle similar clients from anywhere in the world.

Flashpoint PSI is a user-friendly, web-based tool that gives executive protection professionals real-time access to risk intelligence originating from social media and deep and dark web sources.

Reduce Blind Spots to Improve Executive Safety

For executive protection teams, a physical security detail only addresses some risks. Now that security threats happen through both real-world and digital channels, online data is necessary to provide the context to stay ahead of executive threats. Without the right online search tools, your security team could overlook key information for threat detection and response.

With an open-source intelligence solution like Flashpoint PSI, your team can detect threats early on, develop an informed response, and avoid the blind spots that cause executive harm.

What are online communities saying about your Key personnel?

ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, 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 physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams—rely on the Flashpoint Intelligence Platform, comprising open-source (OSINT) and closed intelligence, to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

Learn more at flashpoint.io.

Learn more about our solutions

Book a Demo