



Improving Risk Response For Transportation Security With OSINT

NOTE: Due to the sensitivity of this use case, all organizations, usernames, URLs, locations, and other identifiers are redacted for confidentiality.



How OSINT Supports Critical Transportation Infrastructure

National transportation networks, including airports, seaports, and highways, make up a country's critical infrastructure. When this infrastructure is compromised, governments and security teams need to be prepared and well-informed to prevent damage to assets, data, and human life.

Online data plays a crucial role in providing the information required for transportation security planning and incident response. For intelligence teams, social media networks and deep and dark web content can:

- **Provide the earliest alerts** for location-based threats near airports, seaports, and other transportation hubs
- **Inform security teams about tactics used** to bypass security systems or commit attacks, particularly at airports
- **Monitor for threats directly targeted** at the security/public sector organizations themselves
- **Stay alert to vulnerable data** that could compromise a transportation network's digital or physical security

10

Firearms intercepted by the TSA in 2020 per million passengers—double 2019's rate¹

14%

Percentage of bomb threats targeting transport hubs in 2019²

#3

Transportation's ranking for the most cyber-targeted industry worldwide³

Specialized open source intelligence (OSINT) software is required to efficiently locate this information. But many commercial solutions frustrate security personnel and intelligence analysts working in transportation: some tools are complex and clunky to use and lack the data coverage required to surface risks on hidden sources.

These gaps have serious impacts on transportation security initiatives. Analysts may overlook critical risk indicators, either because they are unable to fully utilize a complex tool, or because the software overlooks sources (e.g. dark web forums, obscure social networks) where relevant data is hiding.

In the event of a targeted threat, missed context could put the public at risk and cost millions in damage to transportation infrastructure. When it comes to cyber risks, it could also cost governments millions in damages, system downtime, and compliance fines—not to mention the loss of public trust.

¹ Transportation Security Administration: "TSA firearm catch rate doubles in 2020 - highest in the agency's 19-year history," tsa.gov, January 2021.

² United States Bomb Data Center: "Explosives Incident Report 2019," USBDC, pg. 13.

³ IBM IRIS: "X-Force Threat Intelligence Index 2020," IBM, February 2020, pg. 32

Process: Addressing Software Gaps With Flashpoint

challenge

- Identify and investigate threats to national transportation networks with the support of online data
- Use OSINT software to access data easily and efficiently
- Ensure sufficient data coverage to avoid overlooked threats

solution

- OSINT software providing access to a wide range of surface, deep, and dark web data
- An intuitive platform enabling fast and easy threat detection

results

- Risks are accounted for on more covert online sources
- Analysts can develop more effective and timely threat intelligence
- People, assets, and data are better protected

To put this use case to the test, analysts were tasked with completing a digital risk assessment for a transportation security organization. The goals were to:

- **Identify current adversary tactics** for bypassing security systems, such as scanners
- **Monitor for on-the-ground security risks** at specific transportation hubs
- **Locate risks and data disclosure** directly targeting or implicating the organization

Analysts used Echosec—Flashpoint’s open-source intelligence solution—to scan hundreds of online sources for actionable threat indicators. These included social media sites, obscure social networks and messaging apps, and deep and dark websites. Users compiled timely information using quick searches, and also set up saved searches to monitor for new risk indicators in real-time.



Results: Exposing Threat Tactics and Early Risk Indicators

1

Bomb threat indicators located via social media near a target airport

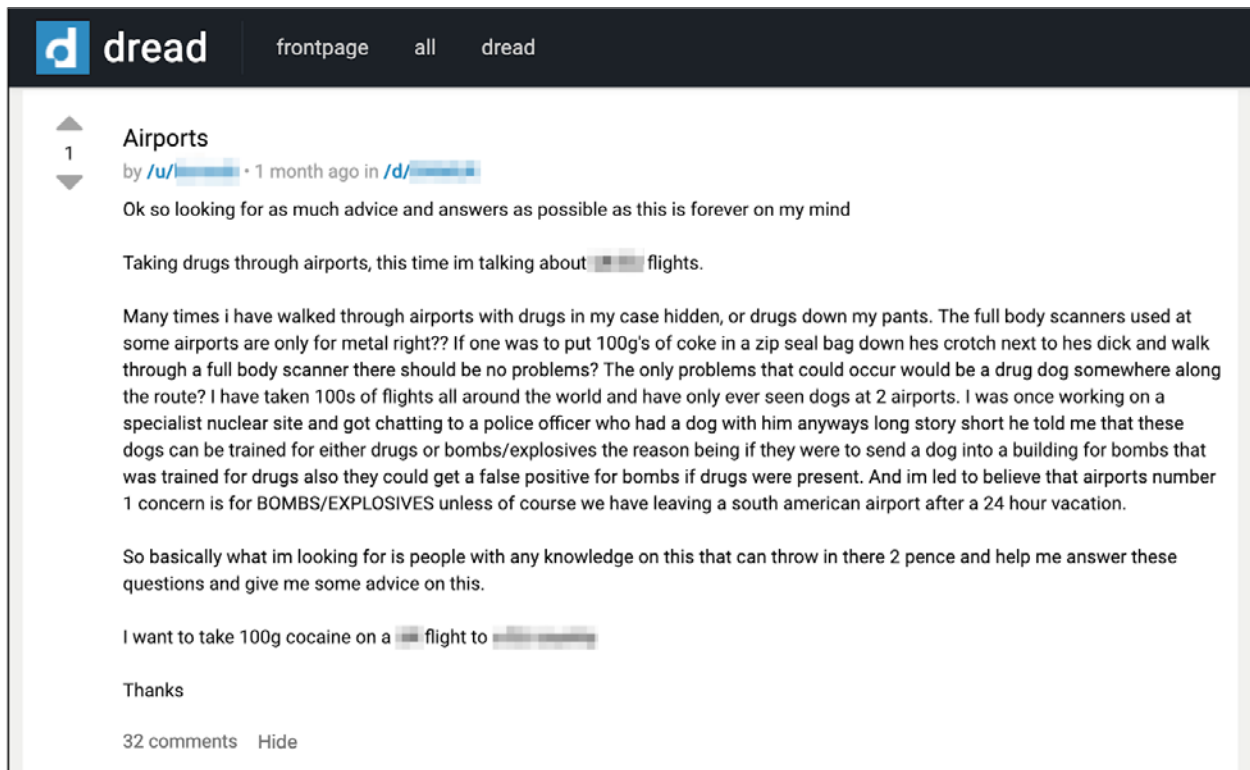
2,650

Known breached records linked to the organization's email domains

Over the course of the assessment, analysts identified:

CURRENT ADVERSARY TACTICS

- Numerous discussions, primarily on deep and dark web forums, describing how to bypass airport security—specifically for smuggling drugs and weapons.
- Dark web vendors selling passports that claim to bypass security scanning systems.

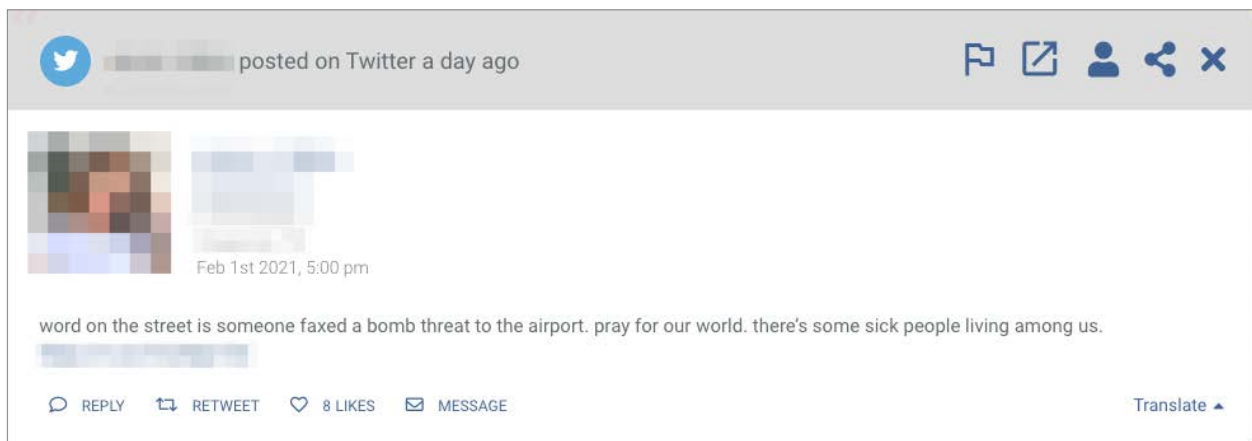


The screenshot shows a forum post on the 'dread' website. The post is titled 'Airports' and is the first post in the thread. It was posted by a user with a blue profile picture, one month ago, in a subforum with a blue header. The post content discusses airport security, specifically mentioning full-body scanners and drug smuggling. The user asks for advice on how to bypass these scanners, mentioning a specific technique of hiding drugs in a zip seal bag. The post also mentions that the user has taken many flights and has only seen drug dogs at two airports. The user concludes by asking for help in finding someone with knowledge on this topic to assist with their request. The post has 32 comments and a 'Hide' button.

Example: Airport smuggling discussion on a dark web forum

PHYSICAL SECURITY RISKS

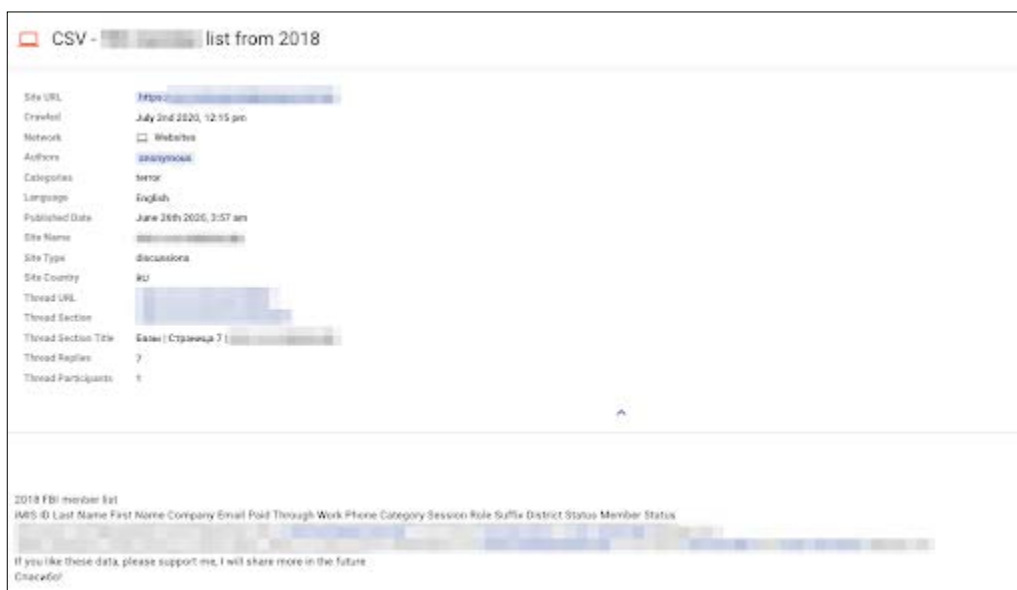
- The use of certain key phrases to obfuscate discussions about targeting airports (e.g. smuggling weapons, stealing/hijacking planes). While these aren't necessarily valid threats, online communities often engage in gamifying or fantasizing attacks, which can motivate real intent.
- Early detection of risks (e.g. fires, bomb threats) geotagged near a specific airport.



Example: Bomb threat indicator geolocated near a target airport

DATA DISCLOSURE

- Numerous posts on deep and dark web paste sites leaking personal identifiers for organization staff, in some cases disclosing passwords. This information could be used to compromise both cybersecurity or the physical safety of staff members or offices.
- Articles mentioning the organization on a dark web, right-wing extremist website.



Example: Staff data leak identified on a Russian deep web forum

Outcome: Usability + Wide Data Coverage = More Informed Risk Response

What set this investigation apart from typical capabilities of other OSINT software?

- **Analysts accessed a wide breadth of relevant data sources**, including social media networks, messaging apps, breached data repositories, and obscure deep and dark websites in one interface. This minimized the need to pivot between multiple tools specializing in, for example, social media or dark web data but not both. Analysts saved time and had access to more context than would be available by analyzing sources in separate tools.
- **The investigation accounted for specialized sources that may not be included in other solutions.** For example, some of the niche networks where risk indicators occurred may have relied on proprietary crawlers, returning data unavailable through other commercial software.
- **Analysts could return relevant data faster than more complex, click-heavy solutions.** Searches were built with the same amount of time and effort required to run a Google search, and analysis and triage were assisted with the use of AI-powered threat classifiers.

With these capabilities, transportation security professionals and analysts have faster and easier access to wider data coverage, supporting timely and exhaustive threat intelligence cycles. This enables more informed decision-making for transportation security initiatives, potentially reducing damages to assets and at-risk populations.

Major transportation hubs, and the entities responsible for their security, now face a variety of digital and physical security risks. These risks are detectable and enabled by an overwhelming variety of publicly available web spaces—in fact, more variety than is typically available in most commercial OSINT tools.

Software usability and data coverage will likely become a primary consideration for security and intelligence teams protecting transportation networks, especially as borders reopen and travel recovers from COVID-19. After all, when a country's critical infrastructure and citizens are at risk—shouldn't intelligence teams have the easiest, most comprehensive access to reliable information?

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 www.flashpoint.io.

Learn more about
our solutions

[Book a Call](#)