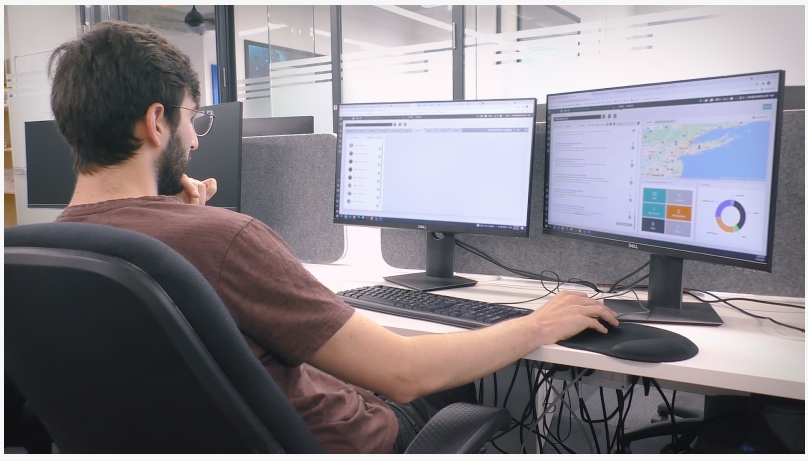
How Data Can Help Border Agents Overcome 6 Threat Intel Challenges

Organizations that can't harness data effectively can't realize its potential to expose threat actors and their networks.



NEW YORK, NY, UNITED STATES, October 6, 2021 /EINPresswire.com/ -- The arrival of threat actors at the United States border has been an issue at least since the nation's boundaries were confirmed with the Treaty of Paris in 1783.

Things are a bit different today, but perhaps only in volume and modes of transport. A bevy of boats, motor vehicles, trains, and aircraft brings millions of travelers to U.S. border crossings and ports of entry. The task for border agents, of course, is to identify and separate the threat actors from the crowds of innocuous families, vacationers, and businesspeople – not an easy assignment even in the best of times. The current environment, as it happens, features the complications of a global pandemic, mass movements of displaced persons, and the ongoing danger of drug cartels, gangs, and terror groups.

The efficient collection and processing of threat intelligence becomes a must for protecting the nation's boundaries. But border agents must confront numerous challenges in doing so. Here are the top six with a few observations on methods and practices for overcoming the obstacles.

1. Identity deanonymization

The key query at the border is whether the person wanting to enter the U.S. is who they claim to be. That's perhaps the ultimate in frequently asked questions. In 2020, a year in which COVID-19 curtailed travel, the U.S. Department of Transportation documented more than 93 million land border crossings.

Most checks are routine, of course. But threat actors' ability to mask their identities in the online world makes for some complicated outliers. Fake accounts abound on well-known and widely used social platforms, forums, and websites, providing threat actors with a degree of anonymity. A threat actor may also link his or her bogus account with other fake accounts to create the appearance of legitimate connections. This activity occurs on the surface web of indexed websites and everyday use. Threat actors, however, can burrow into the deep and dark web layers, which are not indexed through conventional search engines. Here, sophisticated users can employ anonymizing browsers and proxy servers to better conceal identities and achieve a much higher level of anonymity.

Border agents, however, can deanonymize identities. This process involves making connections among pieces of information obtained from the surface web and the internet's underground tiers. Even savvy threat actors end up leaving digital footprints in their online journeys. An email address or phone number may link a threat actor's activity on a dark website to a social platform on the surface web, for example. WEBINT, or web intelligence, provides a structured way to collect and analyze data gleaned from the various web layers. To build such intelligence into an organization's set of investigative methods, a border agent will need insight into how the dark web works and some tools such as specialized browsers for accessing otherwise hidden websites.

Increasingly, automation plays a role in augmenting threat intelligence methodologies. Manual searching and analysis across the multitude of surface and dark websites quickly become time-consuming and untenable amid the volume of travelers that agents must process at border crossings. Automated methods, however, let an individual investigator comb through vast amounts of information in a reasonably short amount of time.

2. Determining network connections

The ability to analyze social connections can serve as one of the most powerful investigative methods for agents protecting the border. This approach sheds additional light on a threat actor. In some cases, a threat actor's lack of social connections could indicate a fake identity. For example, a conjured social profile will often follow many accounts but have few followers. A barrage of newly created connections could also flag a fake identity, since a threat actor may hastily concoct a few "friends" to create a fictitious backstory.

In other cases, however, social analysis helps to uncover a threat actor's broader network, which

could include gang, cartel, or other threat-group affiliations. Here again, automation can help accelerate the investigation methodology, enabling agents to quickly and accurately identify the would-be entrant's associates and the risk they pose to the homeland.

Agents can also use social analysis techniques to zero in on smuggling operations. Threat actors across the border have taken to messaging apps, where they use social engineering to identify likely collaborators in the U.S. Threat actors use the promise of quick cash to entice their targets — teenagers from low-income families, for example — to pick up and transport people coming from across the border. Officials can disrupt such transactions if they can determine where the recruitment is happening online and keep tabs on suspicious activity.

3. Analyzing big data

Organizations that can't harness data effectively can't realize its potential to expose threat actors and their networks. Border agents must be able to sift through massive amounts of data when processing people and cargo — and discover the telling bits of data that make all the difference. The mission for investigators: turn the big data problem into a big data advantage.

Agencies need a plan and a repository to ingest and analyze data. But to target the right data, they also need to create a dictionary of specific keywords, search terms, and objects that reflect the investigative priorities of a given jurisdiction. The terminology will differ from one area to another based on active threat groups, locally used languages, and regional colloquialisms, among other factors.

The dictionary helps automate the process of searching for the critical pieces of data in a threat investigation. A generalized parsing of data won't work. The search criteria contained in the dictionary must be highly specific. This necessity calls for more than methodological rigor and technical capability: Organizations will need to tap into the institutional knowledge that only highly experienced border agencies will possess.

Read the complete article at Hstoday.us:
https://www.hstoday.us/subject-matter-areas/customs-immigration/how-data-can-help-border-agents-overcome-6-threat-intel-challenges/

Johnmichael O'Hare
Cobwebs Technologies
079-6981083
email us here

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.