SHADOWDRAGON

OSINT success hinges on collecting relevant data

A targeted approach that respects individuals' privacy is crucial for turning reliable information into intelligence

Jonathan Couch
ShadowDragon

Open-source intelligence has been around for a long time, but in the past decade or so, it has become even more valuable. On social media, video-hosting sites, web forums, apps, gray literature and news sites, millions of terabytes of data are being created each day, the bulk of which is either commercially or publicly available. Couple that with greater computing power and more connected devices, and the challenge becomes how to synthesize, visualize and translate data into actionable intelligence.

Industry has been supporting a drive to modernize OSINT solutions to help government agencies gather publicly available information (PAI) from disparate sources and display and organize it in a way that allows users to uncover connections between pieces of information that were otherwise hidden.

Choosing which open data sources are relevant depends on the agency's mission and goal. For example, the military would look for places where adversaries are talking about information they shouldn't be sharing. In Ukraine, many members of the Russian army use Telegram to communicate with their friends and families. Russians post where they are and what they're doing, and the Ukrainian army has taken advantage of that in creative ways.

For example, Ukrainian soldiers and women have used dating apps to lure Russians into posting pictures that reveal their location, which can be combined with other location data that is readily available with the right OSINT tools.

Unfortunately, the U.S. has just as many young warfighters who post information online that can be detrimental. The U.S. military has learned a lot from Ukraine. At the National Training Center in Fort Irwin, Calif., soldiers are taught that cell phones will get them killed.

> "Our technology is fully auditable, which means we can reconstruct a user's investigatory journey from start to finish."

Uniquely modern sources of intelligence

Users start by clearly defining the question they want to answer or the challenge they need to tackle, and then they collect information or raw data. Turning that data into actionable intelligence requires taking it through an analytical process that is targeted to a specific problem.

Gathering information about known threats

ShadowDragon helps with the collection and organization of PAI so users can turn it into actionable and valuable intelligence for their specific use case. Our company founder, Daniel Clemens, has a saying that "the more you know, the luckier you are." We apply that philosophy to OSINT by gathering enough data to give investigators and analysts

iStock

the ability to either prove or disprove a hypothesis.

We are strong supporters of ethical OSINT. We do not violate people's privacy. Furthermore, we do not apply artificial intelligence during our collections. Our technology is fully auditable, which means we can reconstruct a user's investigatory journey from start to finish so that law enforcement or other authorities can source every data point without risk of AI hallucinations.

If a system runs vast amounts of data about random people through an AI engine using proprietary algorithms, there is a high chance of generating bad information or targeting somebody who shouldn't be targeted depending on the data the system was trained on or with. Instead, ShadowDragon emphasizes a target-centric approach. We begin with what the threats are and then gather more information about them. For example, we identify a person who is known to be a threat and search for more information to support an active investigation.

Privacy is an ongoing area of concern for the government and the public. ShadowDragon can help agencies and teams ensure they're leveraging PAI for the good of our government and our country while protecting the rights of individuals. ∎

Jonathan Couch is chief operating officer at ShadowDragon.