Will Bushee Follow
May 4, 2017 · 7 min read

WHAT ARE YOU WORKING ON?

We spend our days focused on finding, harvesting, curating and helping clients develop insights from open source intelligence (or OSINT). If you aren't leveraging OSINT, you are missing large amounts of relevant data that is freely available to you.

OSINT is under-used as a foundational tool for security and risk management. Why is that?

To begin, many professionals are not comfortable themselves in understanding what OSINT is and how they can leverage it. Some do not have the programs in place to allow open source intelligence tools to be built and flourish — they are still chasing events and are reactive in approach.

Others are simply confused. It often seems like we struggle most when we are venturing into the unknown, as we often revert to what we know and what is comfortable.

Making Sense of OSINT

Citi Group said it best a few years ago when they stated simply, that in bringing OSINT to the table to enhance security and risk management:

“n = all and noise in the data is acceptable”

On its face, this seems overwhelming. As a result, many companies and organizations stop without considering things more thoughtfully.

We sleep comfortably under traditional risk management models knowing that we have been able to mitigate, transfer, and accept the risks in our mandate.

We’re able to do what we do best with tools such as access controls, internal fraud detection software, cyber security such as DLP solutions, and working closely with internal groups on compliance to rigorous policy and procedure. Risk management 101 — yes, we all get this.

However, **out of nowhere (if you were not watching for the past 15 years), the world of open source data has become the largest**

accessible database for all to use — period.

And while I could dazzle you with numbers regarding the growth of the data online each day, what you really need to know is this: **If you are not leveraging open sources effectively, you are missing something**!

4 OSINT Tips to Improve Your Business

Here are some tips and thoughts about how OSINT can make your business or organization better:

Tip 1: Start with the data you want in mind and use it as the fuel for your analytics and security/risk management efforts

Recently, we received a frantic call from a major UK consulting firm saying that they had purchased the expensive and capable Palantir analytics platform for use.

Now, Palantir does do great things with data analytics by requiring fuel in the form of data. The firm from the UK realized that to generate amazing analytics from open sources through its Palantir deployment, they needed open source data to pull through the great analytics engine they had purchased which we were able to provide.

At BrightPlanet, we believe that the best process for leveraging insights from OSINT is simple:

Start by harvesting data, then curate the data, then move on to the analytics, then formulate your insights and actions.

Tip 2: Know what signals you’re looking for to set up your data harvesting, curation, and analytics platform properly

For many of our clients, the threat assessment program has already been developed. Clients that have an idea of what the signal (in the noise) looks like and what would represent a low, medium, and high level threat for specific risk categories will be successful in leveraging OSINT in their security and risk management practices.

When clients know this, the entities for successful open source intelligence gathering and analysis can be built more effectively.

For example, a client may be interested in assessing the risk of violent protest by radical activists at upcoming event. Threats can be categorized (based on the client’s own understanding of what constitutes low, medium, and high risk) as:

- **Low —** small number of individuals, acting on their own, known to law enforcement, looking to disrupt the event.
- **Medium —** large number of people rally for the cause and organize attendance at the event, including pre-event planning and logistics.
- **High —** large number of people rally for the cause, led by

extremist influencers, many unknown to law enforcement, and logistics pre-event indicate training on arrest avoidance and making weapons from readily available items.

Knowing these risk categories creates a very specific set of criteria for OSINT harvesting, entity tagging, and data curation. This causes the algorithms in a dashboard to send green, yellow, and red lights to decision-makers and operators. Here's what a harvest and tagging effort might look like based on the threat levels above:

- **Low level**: People talking about the event in a negative way are very few, have few followers, and the followers are remote and of no immediate threat to ongoing operations or security. OSINT harvests suggest no indications of past violence.
- **Medium level**: The core people online for whom data is being harvested have a strong following and they are organized — using social media, websites, and structures such as blogs, meeting minutes, and evidence of strong event planning structure. Strong negative talk, with some talks of threats and strong likelihood of operational disruption, but no evidence of violence.
- **High level**: Similar to medium level above, but OSINT harvests suggest violence is being suggested as a viable option and instructions for violent disruption are being provided to followers in online forums. People likely to be involved are being given information about countermeasures, evading police and law

enforcement. Law enforcement or corporate security will need to proactively prepare for large-scale disruption online and on premises and potentially at large cost to all involved.

Everything we spoke of above is able to be supported and threat assessed through effective open source information collection and curation. What is always required is the threat assessment methodology and rules so that the right data (fuel) is collected, and the proper tagging and analytics thresholds are set in dashboards.

Tip 3: Be Proactive

OSINT monitoring is a constant process.

Once a company or organization has determined thresholds and rules for OSINT harvest, they can set up a system to automatically pull masses of data into analytics engines and set up dashboards that allow them to stay ahead of issues before they become problems.

Take the simplified violent protest assessment we just discussed. The same data and rules for event specific threat assessment can be directed to ongoing assessment.

Are we witnessing more rhetoric day over day, week over week? Is the number of followers for key activists and influencers rising? Where are they located? Is the movement localized or gaining traction in new geographies? Are the methods and groups they want to target the same today as it was 6 months ago? One year ago? Is it a policy change that seemed to cause the escalation or reduction in online threat levels?

Remember: *the ONLY way to generate these insights is with ongoing and active monitoring, comparative scoring, etc.*

Tip 4: Bring Artificial Intelligence in, but Feed It the Right Data

Shouldn’t artificial intelligence platforms be able to do everything we’ve noted above? Can’t we just “turn the bots loose” and let them tell when something is happening? As it turns out, it’s not that simple.

Making the most of AI engines such as IBM’s Watson requires training them on baseline data sets and then letting the neural nets (or whatever learning system is hardwired) learn with a constant feed of information via a thoughtful OSINT harvest. AI engines need a proven data set to support fuel baseline, and then fuel the assessment models you have built as a company or organization.

To make a ‘physical security’ comparison, you need to provide training and conduct a walk-through of a new facility for a security guard, so they understand what would constitute a threat at the new location.

If they don’t know what a threat would be, how could they possibly alert anyone or take appropriate actions? If a reconnaissance soldier is not trained to know what threats look like from distances, or how to best estimate enemy advances based on imagery, how do they assess threat? Answering these questions requires gathering of information, seeing what constitutes threats and not, and seeing it over and over again.

Training an AI system with vetted, harvested OSINT data is no different.

An AI system is a sophisticated analytics engine that learns. However, it cannot simply learn on its own. It needs to be given a path with replicable, verifiable positives and negatives so that it can start to identify patterns on its own.

That happens only with a lot of good data at the inception of an AI-based project.

Take Our Word for It

At BrightPlanet, we started our work in the security and intelligence space, doing mass OSINT harvests for private and public clients, and we remain an industry leader today.

The current state of our technology thrives on the ability of our Data-as-a-Service to help provide you with a data solution. We harvest and curate the right open source data to provide enriched information for use in analytics — to monitor risks and assess threats based on the models you have developed.

Let’s explore how we can support your organization in its mandate to keep people safe, assets secure, and proactively support risk management objectives.

If you have any questions on how we can help maximize your business or organization’s potential with OSINT, tell us what you’re working on. One of our expert Data Acquisition Engineers will guide you through all of your possibilities.

Don’t have a specific project in mind yet but interested in additional information on how OSINT can support risk management? Download our white paper on how to use OSINT to strengthen your risk management framework.

The post How OSINT Strengthens Your Security Risk Management appeared first on BrightPlanet.

Originally published on Wordpress