# Why OSINT Analysts Need to Manage Their Digital Identities

When we talk about the work of gathering intelligence, most people conjure the image of a James Bond-esque spy, infiltrating an enemy organization under an assumed identity. But there's another kind of intelligence gathering, just as important to commercial, military, diplomatic and political operations: open source intelligence, or OSINT for short. OSINT is gathered from publicly available information sources like the news, government documents and social media reports, among others. But in order to be effective, OSINT analysts have to be just as careful about concealing their online identities as clandestine operatives.

Online surveillance is just as prevalent and often more subtle than real-world surveillance. If the OSINT analyst doesn't cover their tracks, it's fairly easy for someone with the resources of a nation's intelligence agency, or even a large corporation, to track down the identity of that analyst as they dig for information. The analyst must wipe away their digital fingerprints, so to speak.

"The digital fingerprint is pretty comprehensive, and there are a lot of things that can go into it. At its most basic level, a digital fingerprint includes information about your hardware and software profile, your network, your location, timezone, etc.," says Nick Espinoza, head of technical solutions at Authentic8. "These are the sorts of things that the analyst needs to change or obfuscate, so he or she can collect information without tipping their hand. And not only that, humans are creatures of habit. So targets can begin to discern, based on your browsing patterns, what sort of demographic you might fall into in terms of age, income, spontaneity, general interests and so on. And in the intelligence space, whether it's on the corporate or public sector side of things, having that level of detail on a user's behavior, hardware, software profile, and everything else, is absolutely detrimental."

Because those fingerprints could potentially identify an OSINT analyst as working for a competitor or a government employee, an adversary could lock down previously available avenues of information.

That's why OSINT analysts need a high level of training in the tools required to conceal their digital identities when gathering intelligence. VPNs, proxies and virtual machines are some of the more commonly known tools, but Espinoza says those only go so far. What's far more effective, says Espinoza, is a remote browser platform like Authentic8's Silo.

"Our company provides a web isolation platform with managed attribution. Essentially, managed attribution obfuscates who you are, what you do, and what you're looking for. A combination of technology and tradecraft need to go hand in hand to enable an analyst to accomplish the mission safely and securely, without compromise," Espinoza says. "We've architected our system to incorporate a lot of tradecraft and to minimize the signals that might indicate someone atypical is looking for a particular subset of information on, let's say, a hacker forum, or a ship spotting blog, etc. Our goal is to enable better tradecraft and skill sets, while reducing the digital signature of these analysts as they go about their job."

Silo is a browser hosted on Authentic8's servers, and it provides an encrypted display of your session when you use it. That means you get a clean slate every time you use the browser. No history, no cookies, no location data, no tracking, no profiles, no targeted advertising. You can save your passwords, but those are stored and encrypted on a different server.

"If you are getting very deep on a particular subject, you want to view it firsthand, and you need to do so safely and securely. And that's where the remote browser comes into play," Espinoza says. "You'll be able to view that source directly as it's originally rendered, and you'll be able to do so without tipping your hand that you're an analyst, because you'll look like a local device close to your target, with local languages and time zones."

Because many times, especially when the OSINT analyst works in a country's security context, what's at stake is a greater mission. They're working to provide military leaders, politicians, and diplomats the most up-to-date, accurate information as possible about geographic, geo-political, or even military circumstances. OSINT analysts need to operate as anonymously as possible to ensure that their sources remain open.

"Changing your IP address, what region you're egressing from, and the signals that your hardware-software profile give off are the critical bare minimum actions required to accomplish your job without really showing your hand," Espinoza said. "Our platform provides that level of customization. And it allows an entry level analyst from any public sector, law enforcement or corporate environment to have an impressive arsenal of tools they can use to reduce those tells."

Because the information they gather could mean the difference between success or failure, life or death, war or peace.