WHAT IS

MANAGED ATTRIBUTION,

AND HOW DOES IT IMPROVE ONLINE INVESTIGATION?

TABLE OF CONTENTS

WHAT IS MANAGED ATTRIBUTION?

While many OSINT researchers recognize the need to avoid tipping off their targets, they're still fuzzy on the specifics of managed attribution.

What is managed attribution? Is it the same as misattribution? How about non-attribution? Can it help me stay anonymous online and conceal my identity? We get these questions from online investigators and researchers in virtually every industry and every part of the world.

In our line of work, we are used to the term “managed attribution,” but there's a lot of confusion out there about what it is and what impact it can have on the success of an investigation.

So, let's unpack what managed attribution really is — and is not.

Defining managed attribution

Managed attribution is the ability to control how the details of your device, browser and browsing behavior are projected to websites you visit. We use the term anonymity a lot to convey the benefit of a managed attribution solution, but it's more about blending in with the crowd and matching the details of your digital fingerprint to look like an average visitor to the website you're on. Nothing to see here, webmaster!

To truly understand managed attribution, let's back up a few steps and define “attribution” itself. In the context of an online presence, attribution refers to all the traceable elements and properties that can help locate and identify a website visitor, their organization and the purpose of their visit. This is a problem for researchers who want to blend in and conceal their online identity because modern browser technology has made online tracking incredibly easy.

You start a digital breadcrumbs trail whenever you open a browser. Sites you visit (and even ones you don't) collect a slew of information about your:

- **Connection:** IP address and provider
- **Hardware:** device type, OS, video and audio cards
- **Configurations:** keyboard and language settings, time zones, etc.
- **Installed software and plugins**
- **Other:** even seemingly random things like battery status to help track us across sessions

Then, there's your behavior online. Every link you click on, every term you search, every post you “like” and every comment you publish gets tracked, cataloged, processed, packaged and sold to advertisers. And while millions of web users have similar devices and search items, browsers can fingerprint based on small inconsistencies and distinct combinations of settings and behaviors that make an online presence unique.

If you're an online investigator, being unique is the last thing you want to be. What you want to do instead is blend in and conceal your online identity and intent. And this is where managed attribution comes in.

Managed attribution isn't the same as mis- or non-attribution

While the three terms sound similar, they employ very different approaches to concealing your online identity.

The idea behind **non-attribution** is the attempt to stay completely anonymous while browsing the web. Organizations try to accomplish this through a combination of DIY and commercial solutions ranging from connecting through the VPN to creating dedicated networks and maintaining "dirty" devices to get their analysts online.

Ultimately, none of these are capable of creating a completely anonymous browsing environment because, as we discussed above, browsers track much more than your IP address. And even that can be revealed if a VPN connection fails temporarily.

Private browsing isn't untraceable

"Private" or "Incognito" browsing modes promise to erase some obvious cookies, but there's a lot of information that's still being tracked, which in the wrong hands, can lead the adversary back to the investigator.

Experts agree that with all the tracking mechanisms built into modern browsers, the idea of non-attribution is quickly becoming obsolete and unattainable. has some barriers to accessibility while being adjacent to the surface web and is typically accessed via the same browsers.

Misattribution can be a bad disguise

Misattribution refers to intentionally misleading your targets (subjects of investigations or adversaries) about who you are and your intentions. Some of the tools used to accomplish this are essentially the same as in non-attribution — connecting through VPN, using private browsing, maintaining "burner" machines, etc. — but misattribution effort mainly focuses on maintaining a false online identity.

Here, too, things can go very wrong very quickly. Even if you spend hours constructing and nurturing a fake profile, a single slip-up can give you away and jeopardize your mission. Plus, while a VPN might disguise your real location and spoof a fictitious one, that alone may not be convincing enough for a sophisticated adversary.

Bad actors can also use all the tools that are available to advertisers to dig deeper when something might seem suspicious. And once they discover that they are being investigated, they could either hide their operations or, worse, retaliate against the researchers with malware and other methods.

Managed attribution helps you blend in and conceal your identity

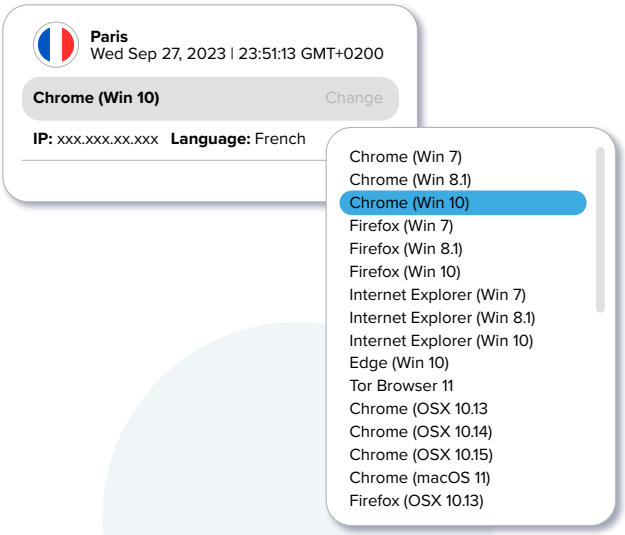
And this brings us to managed attribution — the only way to blend into your environment and conceal your identity during online investigations. With managed attribution, you can completely customize how you appear to sites and people you interact with online by manipulating a variety of device details, including language, time zone and keyboard settings, as well as the browser, OS and other elements.

Using a global egress network, you can adjust your location to appear to be coming from any of dozens of points around the world, showing a local IP address that never refers back to you or your organization.

Purpose-built managed attribution solution

A managed attribution solution like Silo for Research also improves security so digital investigations don't introduce cyber risk. Silo for Research uses a cloud-based web isolation platform that executes all web code remotely, so it never reaches your device and keeps you safe from malware. All evidence is also safely collected, stored, translated and shared through the solution.

With managed attribution working to conceal online identity during investigations, open-source intelligence researchers — from SOC analysts to financial fraud investigators to law enforcement officers — can ensure the integrity of their investigation is maintained and their work doesn't put themselves or their organization at risk.



For more information on how tools like Silo can help you safely utilize the dark web in your investigation, visit our website or request a demo.

silo BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com