Oh, So You Got IOCs? Being a Good CTI Consumer

validhorizon.medium.com/oh-so-you-got-iocs-being-a-good-cti-consumer-ef7e104dbbd6

Daniel Gordon January 20, 2021

Daniel Gordon

Jan 19, 2021

.

3 min read

I wanted to write a blog about being a good consumer of intelligence. I was going to write about the threat intelligence life cycle or understanding your organization to be able to effectively apply intelligence. I was going to write about evaluating sources to identify bias or logical fallacies or reliability of intelligence. I was going to write about intelligence prioritization and why it matters. I was going to write about the value of shared frameworks or taxonomy to communicate information more rapidly and widely.

After having my soul absolutely crushed by world events, here's what I ended up with:

1) Think about what you're consuming. Not only does that mean thinking critically about the content and the source but also think about what impact it's having on you. I don't just mean threat intel either. The shows we watch, the news we read, the social media we participate in, the people we're around all shape who we are and they shape how we see the world. Think carefully about what you read and think carefully about how it's shaping you.

2) Lots of organizations are sensitive about publicly revealing their defensive posture or security maturity for good reason. For miscreants, understanding a victim's defensive capabilities ahead of time is worth its weight in gold. With that said, telling partners what you're interested in and what you're capable of goes a long way toward making their threat intel relevant to you. This is the most critical element of consuming Cyber Threat Intel wine. Kyle also makes the excellent point that some customers don't know what they want which brings up my next point.

3) Know what you want. That means developing an understanding of your organization, people, infrastructure, tools, and processes. Sometimes this is easier said than done, sometimes it's a moving target, and sometimes it's too big for one person, especially when you start thinking about supply chain security. As a customer, you'll never have a good picture of what intel you need unless you have a picture of what you've got.

4) Ask good questions. Be as specific as you can without rambling.

5) If someone shares something helpful, they've done you a favor. Share back if you can.

6) If something is shared with TLP limitations, please respect it, unless of course you're Brian Krebs who sometimes isn't hampered by ethics. My personal opinion is that there are specific situations where TLP can be bent, typically via parallel construction, because of specific risks involved, or because of overly restrictive markings. But here's the thing: You don't get trust back after you lose it. Despite the points made by people who are smarter than me, don't ignore TLP.

7) Automate where it makes sense. I've seen organizations pursuing complete automation of their consumption of threat intel, especially with respect to threat intel feeds. Automation can save a LOT of valuable analyst cycles, but it can also lead to blocking things you need. Careless feeds can include things like 8.8.8.8 or LinkedIn.com or 127.0.0.1, all of which should **not** be on your blocklist. Automate, but do it consciously.

8) Put some work into figuring out if the threat intel you consume is providing value and return on investment. Have your feeds resulted in blocking activity? Are you blocking things that actually present risk? Are you blocking things that are 8 years old?

There are folks who passively ingest threat intel. That's fine and even necessary sometimes for folks who work with classified data or deal with NDAs. But if you want to get more value from your threat intel spend a little time thinking about it, learning/communicating what you

need, giving feedback, and making sure you’re getting good value for the work you put into consuming. And don’t be a jerk to the people that help you.