OSINT vs Paid-for Sources

This lesson will argue the strengths and limitations with intelligence gathered from public sources, and intelligence sold by vendors. We believe that threat intelligence can provide benefits to an organization of any size, but it's important to get the right threat feeds, and consider the size of the budget, if any, for intelligence.

OPEN-SOURCE INTELLIGENCE

There are a ton of great resources to collect free intelligence, but this information needs to be reviewed, and sources should be verified to ensure the intelligence is legitimate and of use. For organizations looking to build out a threat intelligence capability, starting with OSINT sources can be a great way to get used to collecting, analyzing, and utilizing threat intelligence for strategic, tactical, and operational purposes. Free intelligence sources can also be great for independent security researchers that want to provide more context around cyber attacks and activity.

Some great sources of free and open source intelligence include:

- TweetIOC
- Spamhaus
- URLhaus
- AlienVault Open Threat Exchange
- Virus Share
- List of Free Threat Feeds
- Anomali Weekly Threat Briefing
- US Cybersecurity and Infrastructure Security Agency – Automated Indicator Sharing
- SANS Internet Storm Center
- Talos Intelligence – Free Version

PAID-FOR INTELLIGENCE

Purchasing intelligence from vendors can be very expensive, and is likely not a viable option for small to medium organizations. It is typically large enterprises that have dedicated threat intelligence teams that are able to ingest the intelligence and put it to use. But even with a big budget, intelligence can still take a chunk out of it. It's advised to identify what kind of intelligence the organization actually requires, based on the threats that have, or may target, the industries that the company operates in. This is a good idea when purchasing intelligence from vendors such as FireEye, that sell it based on packages relating to different fields and industries.

If you're interested in finding out more about paid-for intelligence, take a look at the sites for some of the giants in this game:

- FireEye
- Recorded Future
- CrowdStrike
- Flashpoint
- Intel471

CONCLUSION

So what is the right choice? Well, it really depends on the organization and factors such as their size, security budget, and need for threat intelligence. We believe that the perfect solution is a mixture of both open-source intelligence and intelligence purchased from vendors. It's still important to question and analyze everything, but once you have sources you know and trust, you can use this intelligence to power defenses, provide context, and take not just a reactive approach to security, but a proactive one.

Previous Topic
Mark Complete
Next Topic
Back to Lesson