How to Gain Better Visibility on Your Infrastructure

Freddy Dezeure
Member of Board of Directors

In my Advisory activity I get to meet many organizations big and small, mature and less mature. Most organizations, even the mature ones, have difficulties to gain sufficient visibility in their networks, obtain high quality threat intelligence and recruit/train/retain qualified CTI and SOC practitioners. When I'm meeting their CISOs I often receive the question on the subject of prevention and detection: "Where do we start?". The answer to that ubiquitous question is invariably: "Get the fundamentals right, first".

Start by improving prevention before investing in detection and hunting. You can best do this by building on best practices in the community. You can use NIST CSF to help you define, implement and monitor the whole of your Security Strategy. You can use guidance from the Centre for Internet Security or by the Australian Signals Directorate to help you setting up and maintaining critical controls. And have a look at the MITRE ATT&CK Framework to capture the latest insights on techniques used by your Adversaries.

In terms of gaining visibility in what happens in your infrastructure I would advise to start by setting up external passive monitoring before investing in SIEMs, sensors and sophisticated log collection and correlation systems. You can learn a lot about your infrastructure by looking at it from the outside. It is an obvious low hanging fruit that is often forgotten.

Compromised machines in your infrastructure are probably calling out to their command and control servers and if these are known by the community they can be taken down or sink holed and confirmed victims could be alerted. When your webpages are infected by malware this will probably be picked up by the search engines scraping them to fill update their search indices. And the owners of the webpages could be alerted about these compromised pages.

When your users compromise their corporate credentials by using them in internet services or social media and these get hacked, you could learn about it by using a credential leak service. When your internet facing services are misconfigured or vulnerable, you can learn about it by using an external scanner.

All these information and alerting services exist, and they don't require any modification of your internal infrastructure. However, most organizations are not aware of their existence, they are not always easy to configure, and their alerts come in different formats and are not always adapted to your internal response mechanisms.

And this is where the products of Arctic Security come in. They make it easy to find those alerting services. And, provided you know your infrastructure (IP and domain ranges), they make it frictionless to subscribe to them and link them to your internal response mechanisms with little or no human intervention. Making low hanging fruits even easier to harvest.