Why Threat Intelligence can be Valuable

If used correctly, threat intelligence has the capability to provide a number of benefits for organizations of any size. Below are a number of examples of how this security practice can provide value to a business by providing in-depth context, prioritization, enrichment, and building a network with other organizations.

CYBER THREAT CONTEXT

While a risk analysis may take a very brief look at the threat actors out there and the chance that the organization will be attacked by them, having a dedicated threat intelligence function could allow the business to perform in-depth research on the threats that are out there, and use historic events and targeting to truly determine what the chances are of being in their crosshairs. Proactive defensive measures can be taken to further reduce the risk, such as giving a vulnerability management team context around the vulnerabilities that are identified during a scan, helping to prioritize patching, and reduce the attack surface.

INCIDENT PRIORITIZATION

Having two incidents occur simultaneously can be draining on resources, and it's crucial that the incident with the highest potential impact is given the right attention and resources so it can be dealt with before damage occurs. Threat intelligence context can potentially give incident responders the information they need to make informed decisions about which incident to prioritize based on the threat actors that have been known to target similar organizations, and by retrieving indicator of compromise enrichment to get as much information from every piece of data.

DIGITAL FORENSICS DOMAIN

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

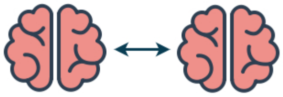
INCIDENT RESPONSE DOMAIN

BTL1 EXAM

INVESTIGATION ENRICHMENT

Giving context to an investigation can make a huge difference. An IP on the internet scanning the organization's public IP range is very common, and normally these IPs are either blocked (if they are sending a high volume of requests) or left alone as the perimeter firewalls are actively blocking them. But, if threat intelligence context states that this IP has been utilized by an advanced persistent threat (APT), such as a foreign nation-state, then this definitely needs more investigation and analysis to see exactly what the IP in question is scanning for.

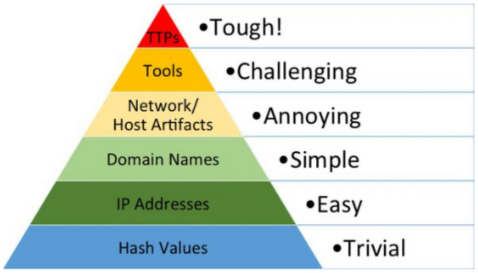
INFORMATION SHARING



Connecting with analysts in other organizations can really help to boost an organization's security posture, by simply seeing how other organizations manage their security and the tools they use. This insight can help the security team make informed decisions based on experience from intelligence sharing partners. It can also help the organization to better defend itself, by receiving early warning signs such as precursors and indicators of compromise, so proactive defensive measures can take place, stopping an attack before it has already begun. We will cover how information can be shared, and in what formats, in the lesson **TI5) Strategic Threat Intelligence, IOC/TTP Distribution**.

PYRAMID OF PAIN

The Pyramid of Pain, which we will cover in more detail during the **TI3) Operational Threat Intelligence section**, is an extremely important part of threat intelligence. Each level of the pyramid represents different types of attack indicators you might use to detect an adversary's activities and is broken up by how much pain it will cause them when you are able to deny those indicators to them. By denying indicators to malicious actors, we're making it harder for them to operate, potentially reducing their ability to launch successful cyberattacks against the organization.



Source: David J Bianco

‹ Previous Topic
Mark Complete ✓
Next Topic ›
Back to Lesson