arcX Cyber Threat Intelligence 101

Day 14/365

13/2/2025

What is Cyber Threat Intelligence?

- CTI is the gathering of information from various sources about current or potential threats to an organization
- But there isn't one single answer, many different things for different people
- Attacker vs Defender

CSec nearly always a defensive activity
The defender must move at the speed of the threat
framework, corporate knowledge, own experience critical for delivering critical advice to your defenders (A structure is the container of creativity)
Not guessing, structure thought

CTI is fundamentally about people interacting with people
almost an exercise in sociology, essentially studying people through the medium of technology

CTI according to Stewart Bertram = at its core, a structured analysis of the threat, the structure exists in your mind and in the tools you are using

Intelligence work is an

- Art
- Craft
- Science

Emergent field within Cybersec

CTI usually sits within a wider Cybersec framework, accompanied by (e.g.) Incident Responders, SOC Analysts,
In addition, the Cybersec framework sits within a wider business context assuming not in an academic setting
You, as threat intelligence, don't exist in isolation.

The word cyber

The word 'cyber' denotes a relationship with information technology (IT), i.e., computers. (It can relate to all aspects of computing, including storing data, protecting data, accessing data, processing data, transmitting data, and linking data.)

The word 'cyber' carries the following connotations:

- A relationship with modern computing (i.e., the digital age). (For example, early computers and home PCs from the 80s and 90s do not attract the term 'cyber.')
- A relationship with the cutting edge of modern technology. (For example, IT security sounds more routine than cyber security, which implies a guard against the latest attack types.)

Cyber both a technological and a cognitive space
The internet is not a homogenous space

Internet iceberg analogy

surface deep and dark levels

surface web - via google
deep web - via normal web browser but more hidden (doesn't mean malicious)
dark web - a section of the internet only accessed using special technology

note that the dark web is not the "elevated digital hell" that modern and pop culture makes it sound like
more like the digital wild west.

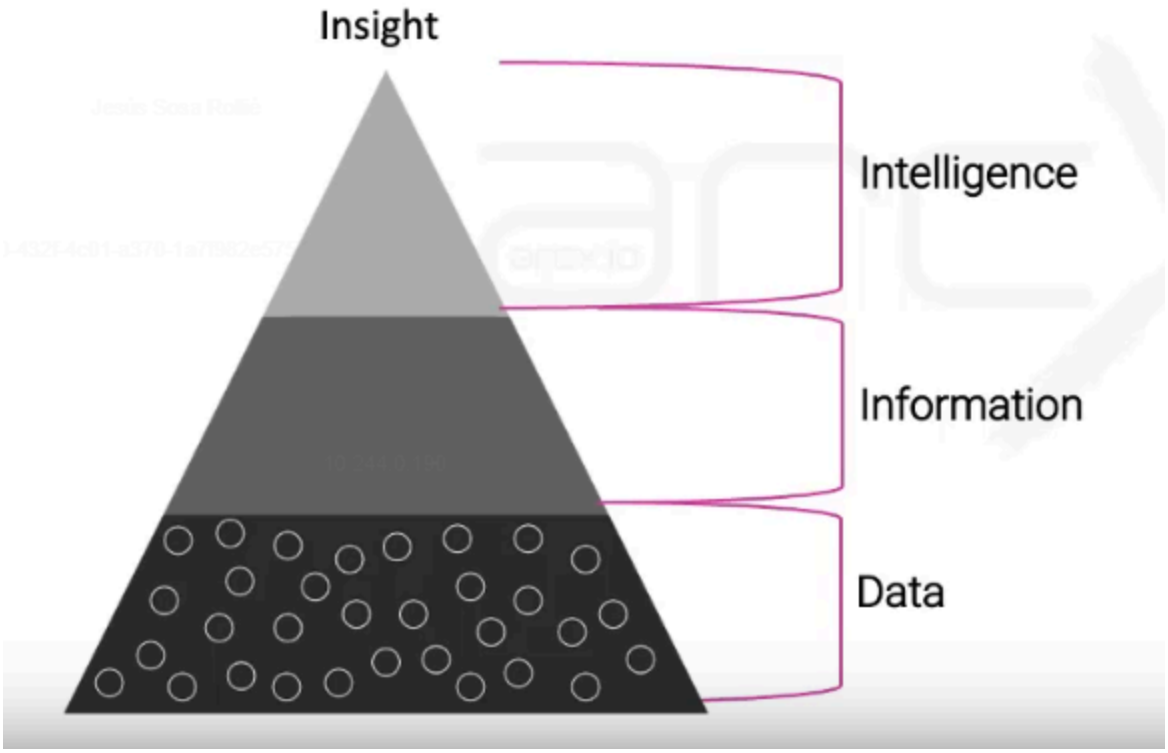
Threat

- a person or thing with the ability to inflict damage onto a victim

---

Intelligence

- Insight an organisation uses to understand the threats they face
  This insight is used to mitigate the harm that an adversary might inflict



Information pyramid, how "intelligence" is produced

- Data refers to simple facts that tend to be available in large volumes, in the context of cybersec IP addresses or log files are examples
- Information is produced when tis data is collated to provide a useful output
- Intelligence comes from the processing and analysis of this information and can be used to inform decision making

Collection turns data into information
Analysis turns information into intelligence