Intelligence Life Cycle

Intelligence life cycle

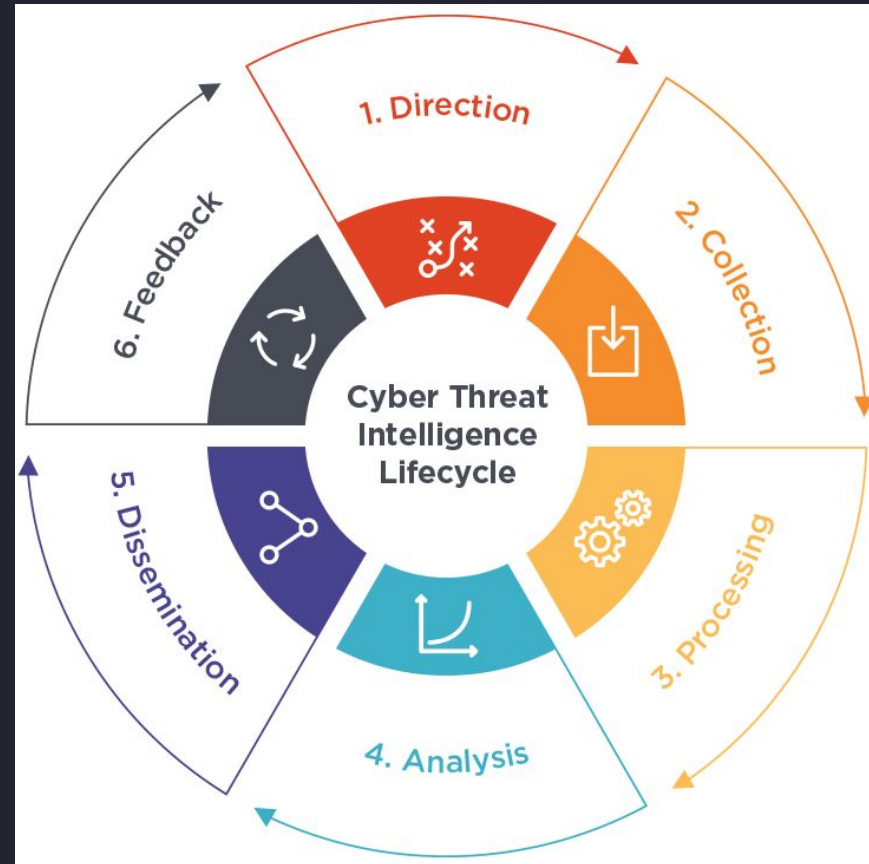**Direction**: Get this information

Collection: I want all the data

Processing: Alright, I don't want that data

Analysis: This interesting when correlated

Dissemination: Here's a report

Feedback: This report sucks

https://www.agari.com/blog/what-is-cyber-threat-intelligence

Direction

Hypothesis generation

Adversary types

Stakeholder assessment

Identification of critical assets

Following Intelligence Requirements.

Collection

Asset integration

Feeds

Raw data parsing

Processing

Transforming the raw data

Correlating and removing

Find Relevance data

Make sure data is Reliable

Being able to process by human or machine

Analysis

Historical relevance

Note formation

Report writing

Dissemination

Finished Intel going out

Different for different teams.

Written reports

Feeds

Automation

Alert creation

Know the consumer

Feedback

Create a plan ahead of time

Discus with consumers

Verify intelligence priorities and requirements of the consumer on a regular basis