Threat Intelligence Collection Management: Understanding Data Reliability

- Analyst must ensure the reliability of data that is collected in order to **achieve better threat intelligence**
- Analyst must **have knowledge** on the various **factors that affect data reliability**

Assessing the relevance of intelligence sources

- The data accessed and collected must be from a reliable source, providing relevant and accurate data
- It must be ensured that this data is not altered during the collection process

Factors affecting the credibility of an intelligence source

- Lack of authenticity of the data accessed
- Inaccuracy of the data provided
- Availability of incomplete or insufficient data

Data collection methods affecting the availability of data

- Different methods of collecting data may bring out a certain amount of data according to the access level
- For example:
  - Passive method only collects internal and open shared data
  - Active method only accesses the authorized level of data only
  - Hybrid method provides the traps-based data collection

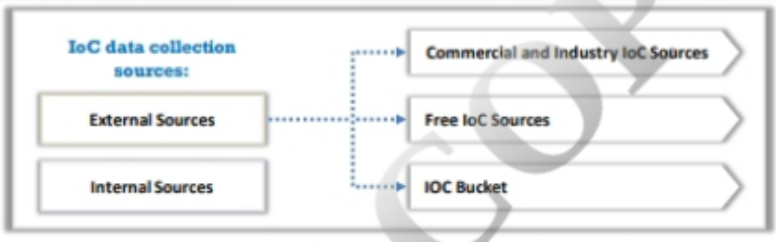
Threat Intelligence Collection Management: Produce Actionable Threat Intelligence

- Utilization of **low cost or free sources** of intelligence may introduce **additional risks** to the organization and compromises the quality of the decision-making process
- Analysts need to concentrate on **selecting intelligence sources** that contain data that is relevant, accurate, timely, and has maximum coverage
- Analysts need to answer the following questions to ensure that the intelligence data is relevant and can produce actionable threat intelligence:
  - Does the intelligence belong to the same geographical location as the organization?
  - Does the intelligence support the strategic business requirements of the organization?
  - To what extent is the information about threat actors, IoCs, and TTPs useful to the organization?
  - What are the broader effects of the intelligence on the organization?

Notes: _____

Collecting IoCs

- Indicators of Compromise (IoCs) are the **pieces of technical data** that are used for **building tactical threat intelligence**
- IoCs are the **clues or forensic evidence** that indicate a potential intrusion or malicious activity in an organizational network
- It comprises information regarding **suspicious or malicious activities** that is collected from various security establishments in a network infrastructure
- IoCs assist the analyst in knowing "**what happened**" in the attack and helps the analyst to observe the behavior and characteristics of malware



Create an Accessible Threat Knowledge Base

- A knowledge repository or **knowledge base** is an important tool for the management and dissemination of threat intelligence
- The repository helps analysts to document and share threat intelligence during the entire **threat collaboration environment**

Threat knowledge repository must include:

- **Pivoting:** The ability to contextualize threat data and correlate related activities
- **Content Structuring:** The ability to store threat intelligence in a structured format
- **Data Management:** The ability to modify or delete past or irrelevant threat data
- **Protection Ranking:** The ability to apply protection ranking to sensitive data to ensure highly critical data is not shared with untrusted partners
- **News Feeds:** The ability to provide real-time news, alerts, briefings, and reports
- **Evaluating Performance:** The ability to evaluate past security metrics
- **Searchable Functionality:** The ability to query for and enrich indicators

Notes: