# **Intro to Cyber Threat Intel**

CTI is the process of **collecting, analyzing, and applying** information about potential or current threats to an organization’s digital and physical assets.

**1. Definition**

* **Cyber Threat Intelligence (CTI)**:  
  Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging threat.
* Focuses on helping organizations **understand threats** and **make informed security decisions**.

**2. Purpose of CTI**

* **Identify threats** before they cause harm.
* **Understand attacker methods** (TTPs: Tactics, Techniques, Procedures).
* **Enable proactive defense** and incident response.
* **Prioritize security efforts** based on actual risk.

**3. Key Benefits**

* Improved **threat detection** and prevention.
* Enhanced **incident response** speed and accuracy.
* Reduced **false positives** in alerts.
* Support for **risk management** and compliance.
* Better **strategic security planning**.

**4. Types of CTI**

1. **Strategic Intelligence**
   * High-level, long-term insights for executives and decision-makers.
   * Example: Nation-state threat trends, industry attack forecasts.
2. **Tactical Intelligence**
   * Information about adversary tactics, techniques, and procedures (TTPs).
   * Often derived from frameworks like **MITRE ATT&CK**.
3. **Operational Intelligence**
   * Specific details about ongoing attacks, campaigns, or actors.
   * Example: Current phishing campaign targeting your sector.
4. **Technical Intelligence**
   * Technical indicators like IP addresses, domains, malware hashes (IOCs).
   * Used for security tool configurations (firewalls, SIEM, IDS/IPS).

**5. CTI Sources**

* **Internal Sources**:  
  Logs, SIEM data, past incident reports, vulnerability scans.
* **External Sources**:  
  Open-Source Intelligence (**OSINT**), paid threat feeds, ISACs, government advisories, dark web monitoring.
* **Human Intelligence (HUMINT)**:  
  Insider reports, security researchers, law enforcement.

**6. CTI Lifecycle**

1. **Requirements** – Define what intelligence is needed.
2. **Collection** – Gather data from internal & external sources.
3. **Processing** – Organize, filter, and normalize raw data.
4. **Analysis** – Identify patterns, relationships, and threat context.
5. **Dissemination** – Deliver intelligence to stakeholders.
6. **Feedback** – Review and improve intelligence processes.

**7. Common Threat Actors**

* Nation-state hackers (APT groups)
* Cybercriminal gangs
* Hacktivists
* Insider threats
* Script kiddies

**8. Challenges in CTI**

* Information overload (too many threat feeds).
* False positives and irrelevant alerts.
* Rapidly changing threat landscape.
* Attribution difficulties (who is behind the attack?).

**9. CTI Tools & Frameworks**

* **MITRE ATT&CK** (TTP mapping)
* **STIX/TAXII** (Threat intel sharing formats)
* **MISP** (Open-source threat intel platform)
* Threat intelligence platforms (**TIPs**) like Anomali, ThreatConnect.

**10. Key Takeaways**

* CTI is not just about collecting data — it’s about **actionable insights**.
* Intelligence must be **timely, relevant, and accurate**.
* Collaboration and sharing improve CTI effectiveness.