

Introduction to Cyber Threat Intelligence

Introduction to Cyber Threat Intelligence (CTI)

Purpose: Provide a concise, easy-to-read overview for students, analysts, or anyone new to the field.

1. What Is Cyber Threat Intelligence?

Aspect	Description
Definition	Actionable information about current or emerging threats that helps organizations understand, prepare for, and respond to cyber risks.
Goal	Turn raw data (e.g., logs, alerts) into knowledge that informs security decisions and reduces risk.
Key Question	<i>Who is attacking? What are they after? How are they doing it? When and where might it happen?</i>

2. Types of Threat Intelligence

Tier	Name	Typical Consumers	Example Output
Strategic	High-level, business-focused insights	Executives, board members, risk managers	Threat landscape reports, geopolitical risk assessments
Operational	Details about specific campaigns, tools, or threat actors	SOC teams, incident responders	Malware signatures, phishing kit analysis, attacker TTPs
Tactical	Technical data that can be directly applied to defenses	Security engineers, threat hunters	IOC lists (IP, hash, domain), YARA rules, Snort/Suricata signatures
Technical (sometimes merged with Tactical)	Raw data feeds, sensor outputs	Automation platforms, SIEMs	NetFlow records, DNS query logs, raw packet captures

3. The CTI Lifecycle (The “INTEL” Process)

Introduction to Cyber Threat Intelligence

1. Planning & Direction

- Define intelligence requirements (e.g., “Identify ransomware groups targeting healthcare”).
- Prioritize based on risk appetite and business impact.

2. Collection

- Sources: open-source (OSINT), commercial feeds, internal telemetry, dark web monitoring, vendor sharing platforms.
- Tools: web scrapers, threat intel platforms (TIPs), honeypots, threat share communities (e.g., MISP).

3. Processing & Exploitation

- Normalize data (STIX/TAXII, CSV, JSON).
- De-duplicate, enrich (add context like geolocation, attribution).

4. Analysis

- Apply frameworks (MITRE ATT&CK, Diamond Model, Kill Chain).
- Identify patterns, assess credibility, estimate impact.

5. Dissemination

- Formats: reports, dashboards, alerts, STIX/TAXII feeds.
- Tailor content to audience (executive summary vs. technical IOC list).

6. Feedback & Review

- Capture lessons learned, adjust requirements, improve collection methods.

4. Core Frameworks & Standards

Framework	Use	Key Elements
MITRE ATT&CK	Mapping adversary behavior to techniques	Tactics, Techniques, Sub-techniques, Mitigations

Introduction to Cyber Threat Intelligence

Framework

Use

Key Elements

Diamond Model	Understanding relationships among four vertices	Adversary, Capability, Infrastructure, Victim
Lockheed Martin Cyber Kill Chain	Visualizing attack phases	Recon ? Weaponization ? Delivery ? Exploitation ? Installation ? C2 ? Actions on Objectives
STIX/TAXII	Structured sharing of CTI	STIX (data model), TAXII (transport)
VERIS	Quantifying breach impact	Actors, Assets, Actions, Outcomes

5. Sources of Threat Intelligence

Category Examples Strengths Limitations