

Introduction to Cyber Threat Intelligence (CTI)

TEJAS MHASKE
CYBER SECURITY TRAINER

What is cyber threat intelligence?

“Intelligence is information that is received or collected to answer specific questions on who, what, where, when, how and why...”

UK National Crime Agency (NCA)

“Intelligence is knowledge and foreknowledge of the world around us – the prelude to decision and action...”

US Central Intelligence Agency (CIA)

Frequently, risk is defined as a combination of threat, vulnerability and impact.

Threat is defined as the intent and capability of adversaries to target an asset

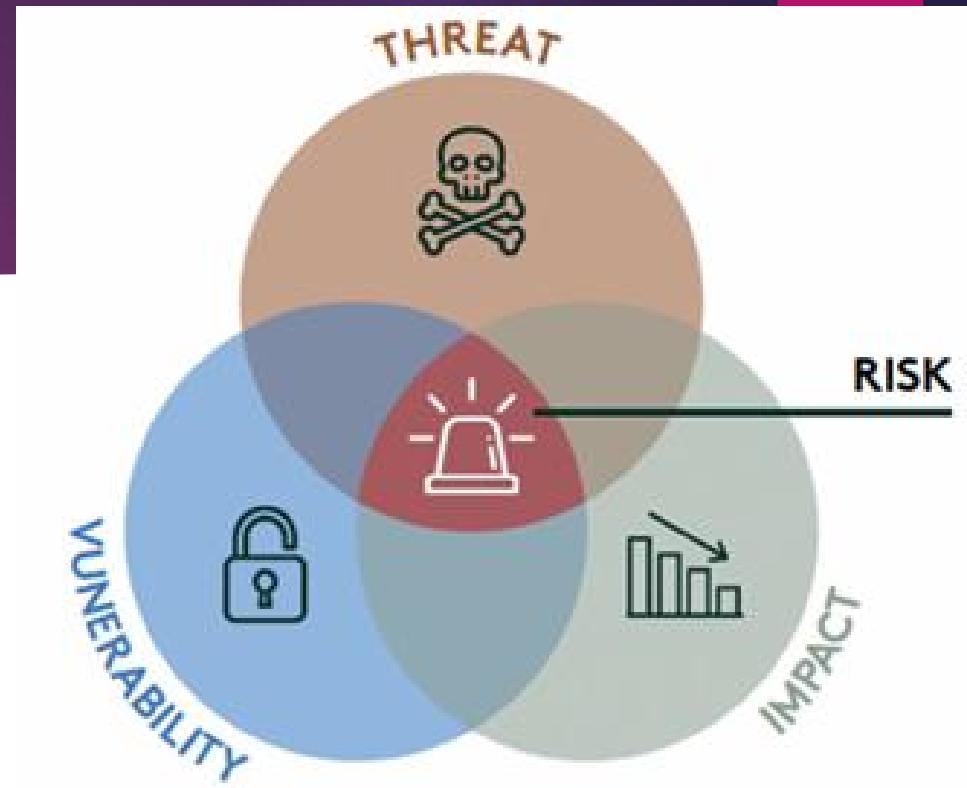


Figure 1: Frequently, risk is defined as a combination of threat, vulnerability and impact

Importance of CTI in Cybersecurity

1. Proactive Defense:

CTI helps organizations predict and prevent attacks before they occur by identifying emerging threats.

- **Example:** Detecting phishing campaigns targeting employees through email analysis and blocking malicious domains.

2. Informed Decision-Making:

CTI guides decision-making by prioritizing critical threats and resource allocation.

- **Example:** An e-commerce company focuses on securing payment systems after intelligence reveals increased attacks on online transaction platforms.

3. Enhanced Incident Response:

Quick access to threat intelligence improves response times during active attacks.

- **Example:** During the SolarWinds breach, organizations with CTI tools identified and isolated compromised systems swiftly, reducing the scope of damage.

4. Awareness of Evolving Threats:

Continuous monitoring of threat landscapes keeps organizations updated on tactics used by adversaries.

- **Example:** Tracking advancements in ransomware-as-a-service (RaaS) platforms like Conti.

The intelligence cycle

- The intelligence cycle is the process by which raw data and information is identified, collected and then developed into finished intelligence for use by decision makers



Planning and direction

- ⦿ Planning and direction is the first phase of the intelligence cycle.
- ⦿ It is used to coordinate intelligence activities to most efficiently serve the consumer's requirements, and should involve significant interaction between the consumer and producer.
- ⦿ This phase should determine the exact requirements of the consumer - often called intelligence requirements (IRs) or priority intelligence requirements (PIRs).
- ⦿ From these IRs and PIRs, one can establish what data and information is required and how it should be collected. This output is often codified in an intelligence collection plan (ICP)

Collection

- ⦿ The second phase, Collection, involves gathering the data and information that is likely to meet the identified requirements.
- ⦿ This will typically involve collecting from a wide array of sources.
- ⦿ Understanding which sources are likely to produce the desired information, be reliable, and provide information that can be consumed in a timely manner, is a complicated process.
- ⦿ It requires good planning and direction to help separate the signals from the noise.

Processing and analysis

- ⦿ Processing and analysis, in which raw data and information is collated, fused with other sources, and turned into intelligence, is the third phase in the cycle.
- ⦿ Human and machine capabilities alike in this phase need to be geared towards answering the IRs for the engagement while adhering to the principles of intelligence .
- ⦿ Analysts will typically apply a variety of quantitative and qualitative analytical techniques to assess the importance and implications of processed information, integrate it by combining disparate pieces of information to identify patterns, and then interpret the significance of any newly developed knowledge.
- ⦿ Analysts are likely to use a range of techniques in order to ensure accurate and unbiased assessments that should be predictive and actionable.
- ⦿ Evaluation of the reliability of the source and the material collected is also applied during this phase.

Dissemination

- ⦿ Dissemination is the timely conveyance of completed intelligence products in an appropriate format to the intended consumers.
- ⦿ The frequency of dissemination should match the time period on which the content is based – for example, operational material needs to be delivered frequently, whereas strategic content will be more intermittent.
- ⦿ Via soliciting feedback and refining existing IRs – or developing new ones – the intelligence cycle can begin again.

Introduction to CTI Frameworks

⦿ What are CTI Frameworks?

- CTI frameworks organize and standardize threat intelligence.
- They help security teams understand, detect, and mitigate cyber threats.

⦿ Why Learn CTI Frameworks?

- To gain insights into attacker behaviors.
- To systematically strengthen cybersecurity defenses.
- To use a common language for discussing threats.

Key CTI Frameworks

1. MITRE ATT&CK:

- ⦿ Focus: Adversary tactics, techniques, and procedures (TTPs).
- ⦿ Application: Analyzing and mitigating attacks.

2. Lockheed Martin Cyber Kill Chain:

- ⦿ Focus: Stages of a cyberattack.
- ⦿ Application: Preventing attacks early in the chain.

3. Diamond Model of Intrusion Analysis:

- ⦿ Focus: Relationships between attacker, victim, infrastructure, and capabilities.
- ⦿ Application: Investigating and responding to incidents.

MITRE ATT&CK Overview

What is MITRE ATT&CK?

- ⦿ A globally-accessible knowledge base of adversary tactics and techniques.
- ⦿ Organized in a matrix format with rows (tactics) and columns (techniques).

Why Use It?

- ⦿ Provides real-world attack data.
- ⦿ Supports systematic defense planning. Widely adopted by organizations globally.

Applications of MITRE ATT&CK

Use Cases:

1. Threat Detection:

- ⦿ Map detected activities to tactics and techniques.

2. Incident Response:

- ⦿ Identify the attack phase and plan mitigations.

3. Gap Analysis:

- ⦿ Assess existing defenses against known techniques.

MITRE ATT&CK Navigator

Tool: MITRE ATT&CK Navigator

[Link to Tool: <https://mitre-attack.github.io/attack-navigator/>]

Scenario: Phishing Attack

1. Open the Navigator and create a new layer.

2. Highlight relevant tactics and techniques:

 1. **Tactic:** Initial Access.

 2. **Technique:** Phishing.

3. Add notes:

 1. "Phishing email tricked a user into revealing credentials."

4. Discuss mitigations:

 1. Email filters, user training, and multi-factor authentication (MFA).



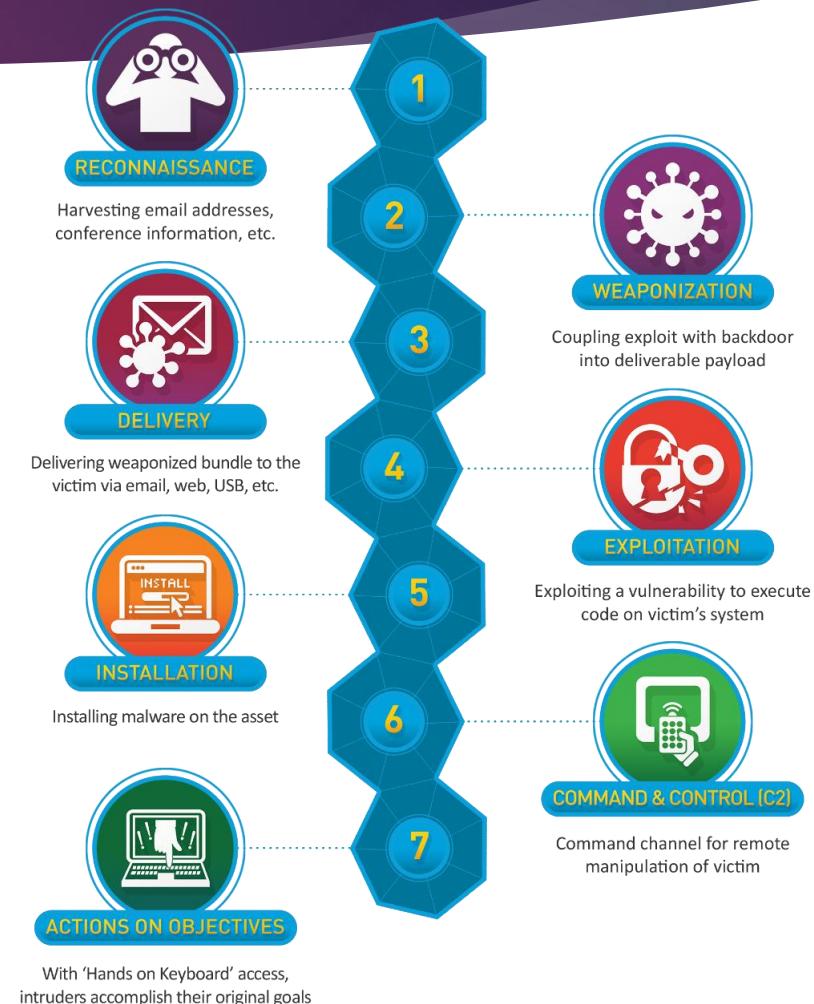
Lockheed Martin Cyber Kill Chain

Stages of the Cyber Kill Chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives

Applications:

- Disrupt attacks at early stages.
- Align defenses to break the chain.



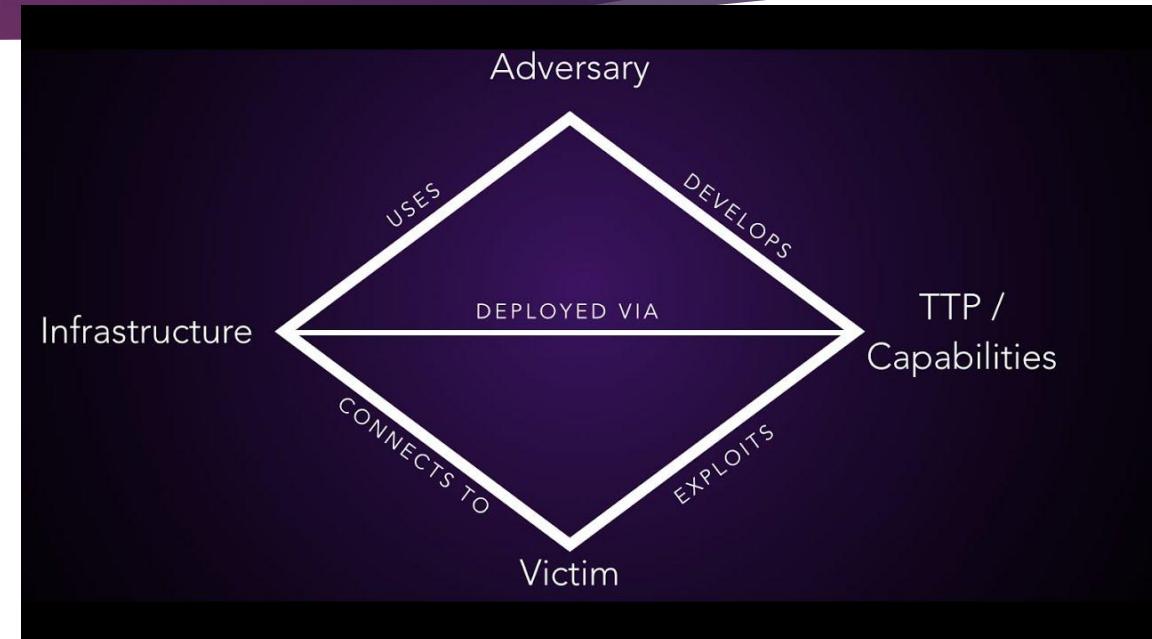
Diamond Model of Intrusion Analysis

Core Components:

1. Adversary
2. Infrastructure
3. Capability
4. Victim

Use Cases:

- Understand attack relationships.
- Support threat hunting and incident response.

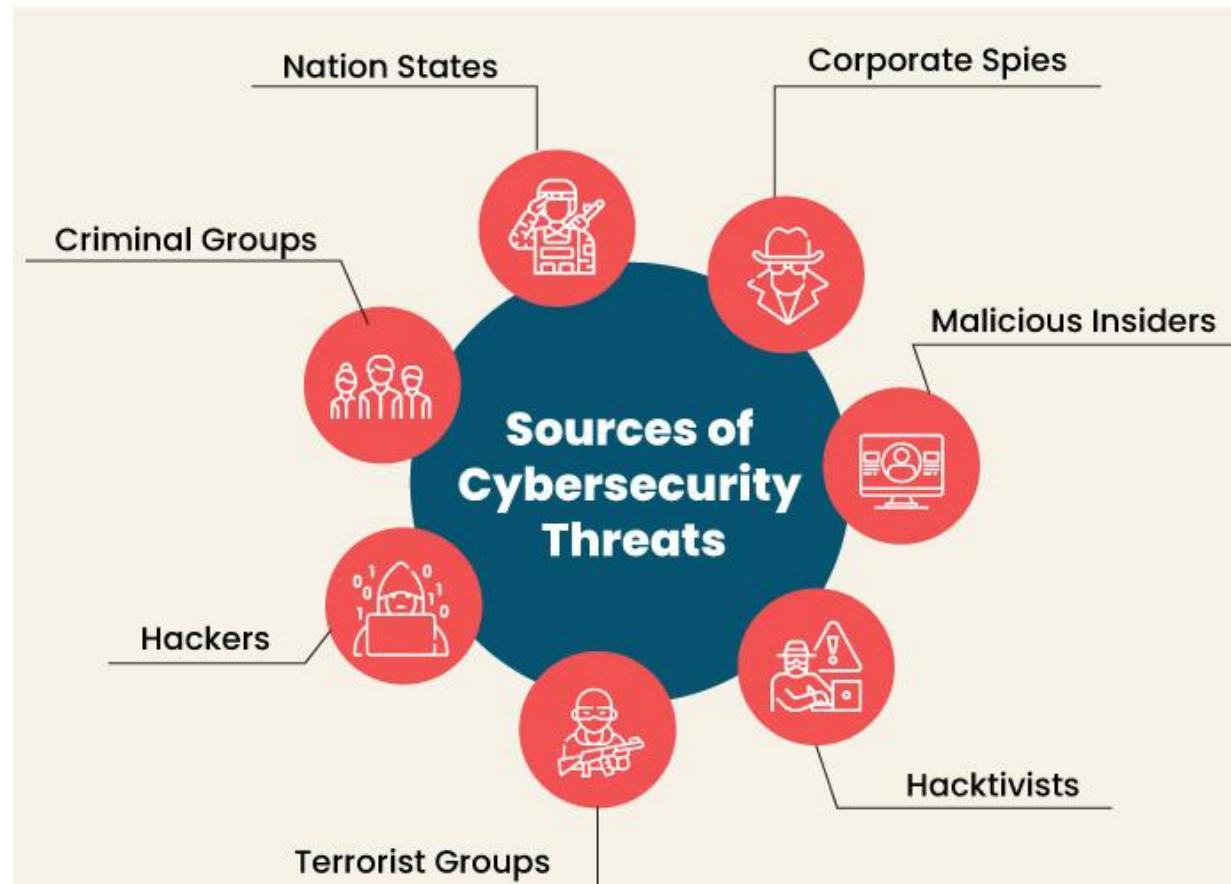


Comparing Frameworks

Framework	Focus	Best Use Case
MITRE ATT&CK	Tactics and techniques	Analyzing attacker behaviors
Cyber Kill Chain	Stages of an attack	Disrupting attack progression
Diamond Model	Relationships in intrusions	Investigating incidents

Threat Actors and Their Motives

- 威胁 actors are individuals, groups, or organizations responsible for cyberattacks.
- They aim to exploit vulnerabilities in systems for personal, financial, political, or ideological gain.
- By understanding these actors and their motives, cybersecurity professionals can anticipate threats and implement effective defense strategies.



Cybercriminals

- Cybercriminals are financially motivated individuals or groups. Their primary objective is to profit from their attacks. They may steal sensitive data, demand ransom payments, or sell stolen information on the dark web.
- **Example:** A ransomware gang encrypts a company's data and demands payment in cryptocurrency to unlock it.
- **Tactics Used:**
 - Ransomware (e.g., encrypting critical files).
 - Phishing attacks to steal personal credentials.
 - Fraudulent transactions using stolen credit card information.
- **Notable Case:** The Colonial Pipeline ransomware attack in 2021 caused widespread fuel shortages in the U.S.

State-Sponsored Actors

- These are sophisticated groups funded and supported by nation-states. They conduct cyberattacks to achieve political, economic, or military objectives.
- **Example:** A state-sponsored group may infiltrate another nation's government systems to steal classified data or disrupt critical infrastructure.
- **Tactics Used:**
 - Espionage: Spying on political or military targets.
 - Sabotage: Disabling critical infrastructure like power grids or water supplies.
 - Disinformation: Spreading false information to destabilize societies.
- **Famous State-Sponsored Group:** *APT29* (Cozy Bear), suspected of being linked to Russian intelligence agencies.

Insiders

- Insider threats come from within an organization, including employees, contractors, or business partners. Insiders often have access to sensitive systems, making their actions especially damaging.
- **Motives:**
 - **Revenge:** A disgruntled employee may sabotage systems after being terminated.
 - **Financial Gain:** Selling sensitive information to competitors or cybercriminals.
 - **Negligence:** Unintentional errors, such as sending sensitive emails to the wrong recipients, can also lead to security breaches.
- **Example:** Edward Snowden, who leaked classified NSA information in 2013, is often cited as an insider threat case.

Terrorist Groups

- Terrorist groups use cyberattacks to promote their ideologies, cause destruction, and instill fear. They often target critical infrastructure, such as power grids, communication networks, or financial systems.
- **Tactics Used:**
 - Propaganda: Hacking social media accounts to spread their message.
 - Infrastructure attacks: Targeting water supplies or transportation systems.
 - Financial disruption: Attacking banks or stock markets to destabilize economies.
- **Example:** Cyberattacks by groups aligned with ISIS aimed to spread propaganda and disrupt Western operations.

Script Kiddies

- These are inexperienced individuals who use pre-written tools and scripts to launch attacks. They typically do this for fun, experimentation, or to gain recognition.
- **Motives:**
 - Testing their capabilities.
 - Gaining attention among peers.
 - Causing minor disruptions.
- **Example:** A teenager using downloadable tools to launch a DDoS attack on a school's website to delay an online exam.

Hacktivists

1. Hacktivists are activists who use hacking as a form of protest or advocacy. They are typically motivated by political, environmental, or social issues.
2. **Example:** A hacktivist group may target a government website to protest policies they believe are unjust. This could involve defacing the website or exposing confidential data to embarrass the organization.
3. **Tactics Used:**
 1. Distributed Denial of Service (DDoS) attacks to make a website inaccessible.
 2. Leaking sensitive emails to reveal alleged misconduct.
 3. Website defacement to display political messages.
4. **Famous Hacktivist Group:** *Anonymous*, known for attacking organizations they perceive as oppressive or unethical.

Competitors

- ⦿ Rival businesses may engage in unethical practices to gain a competitive edge. This can involve corporate espionage, stealing intellectual property, or sabotaging operations.
- ⦿ **Example:** A competitor may hire hackers to steal trade secrets or disrupt the product launch of a rival company.

Motives of Threat Actors

- ⦿ **Financial Gain:** Ransomware attacks, identity theft, and online fraud.
- ⦿ **Political Goals:** State-sponsored espionage or hacktivism.
- ⦿ **Revenge:** Insiders or hacktivists seeking retaliation.
- ⦿ **Ideology:** Hacktivists or terrorist groups promoting their beliefs.
- ⦿ **Curiosity:** Script kiddies exploring hacking tools.

Threat Intelligence Sources and Collection Methods

- 威胁 intelligence involves collecting and analyzing information to identify and respond to cyber threats. This intelligence helps organizations predict attacks, prevent breaches, and strengthen defenses.

Types of Threat Intelligence Sources

1. Open Source Intelligence (OSINT)

- OSINT refers to publicly available information. This can include data from websites, social media, news, forums, and blogs.
- **Example Sources:**
 - Twitter (for real-time updates on new malware).
 - Public databases like VirusTotal (to analyze suspicious files).
 - Forums discussing vulnerabilities.
- **Benefit:** Easy to access and provides broad situational awareness.

Types of Threat Intelligence Sources

2. **Human Intelligence (HUMINT)** HUMINT is intelligence gathered from human interactions, such as engaging with threat actors in underground forums or interviewing industry experts.
 - **Example:** Security analysts joining dark web forums to monitor hacker activity or gain insights into planned attacks.
 - **Benefit:** Direct and actionable insights into ongoing threats.
3. **Dark Web Intelligence** Threat actors often operate on the dark web, selling stolen data, trading exploits, or planning attacks. Monitoring these activities can reveal valuable intelligence.
 - **Example:** Tracking stolen credentials on dark web marketplaces.
 - **Benefit:** Helps organizations detect data breaches early.

Types of Threat Intelligence Sources

4. Technical Intelligence This includes data collected from technical systems and security tools. It focuses on technical indicators of compromise (IOCs) like IP addresses, malware signatures, or unusual traffic patterns.

- **Benefit:** Provides specific details to help detect and mitigate threats.

5. Threat Feeds and Intelligence Platforms Automated tools and platforms provide real-time information about new and emerging threats. These are usually curated by cybersecurity companies.

- **Benefit:** Constant updates ensure organizations stay ahead of emerging threats.

Collection Methods

1. Passive Collection

- ⦿ Involves gathering data without actively interacting with the source. This method is non-intrusive and helps avoid alerting attackers.
- ⦿ Example: Monitoring social media for threat actor discussions.

2. Active Collection

- ⦿ Requires direct engagement with systems or platforms to gather intelligence.
- ⦿ Example: Actively scanning networks to detect vulnerabilities.

3. Collaboration with Third Parties

- ⦿ Sharing threat intelligence with other organizations, governments, or security forums.
- ⦿ Example: Industry-specific Information Sharing and Analysis Centers (ISACs).

Epique