PROJECT REPORT

Name Sudhir S Bhat

Title: **Threat Intelligence (CTI) Gathering and Analysis**

1. Introduction

In today's cyber landscape, organizations are no longer asking "Will we be attacked?" but "When and how will the next attack happen?"
Threat Intelligence helps answer this question by transforming raw threat data into meaningful insights that security teams can act upon.

This project focuses on understanding **Cyber Threat Intelligence (CTI)**—how threat information is collected, analyzed, and used to strengthen an organization's defensive posture. As a intern, this project helped me shift my mindset from **reactive security to proactive defense**.

2. What is Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence is **evidence-based knowledge** about existing or emerging threats that can help organizations make informed security decisions.

CTI answers

- Who is attacking?
- Why are they attacking?
- What techniques are they using?
- How can we detect or prevent them?

Unlike raw logs or alerts, CTI provides **context, relevance, and actionability**.

3. Why Threat Intelligence is Important

Without CTI

- SOC teams react after damage occurs
- Alerts lack context
- Security tools operate in silos

With CTI

- Attacks are detected earlier
- Alerts are prioritized correctly
- Defenses align with real-world threats

Threat Intelligence bridges the gap between **technical data** and strategic security decisions.

4. Types of Threat Intelligence

4.1 Strategic Threat Intelligence

- High-level intelligence for leadership
- Focuses on trends, risks, and geopolitical threats
- Used by CISOs and executives

4.2 Tactical Threat Intelligence

- Focuses on attacker techniques and tools
- Maps threats to frameworks like MITRE ATT&CK
- Used by SOC analysts

4.3 Operational Threat Intelligence

- Details specific campaigns or threat actors
- Includes TTPs (Tactics, Techniques, Procedures)

4.4 Technical Threat Intelligence

- Low-level indicators (IPs, hashes, domains)
- Used for detection and blocking

5. Threat Intelligence Lifecycle

Threat Intelligence follows a structured lifecycle to ensure accuracy and relevance.

CTI Lifecycle Phases

1. Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback

This lifecycle ensures intelligence remains **timely, accurate, and actionable**.

6. Direction (Defining Intelligence Requirements)

In this phase, security teams decide

- What threats matter most?
- Which assets are critical?
- What questions need answers?

Example:

- "Are ransomware groups targeting financial organizations using phishing?"

This step prevents intelligence overload and focuses efforts on business risk.

7. Collection of Threat Intelligence

Threat data can be collected from multiple sources.

7.1 Open Source Intelligence (OSINT)

- Blogs
- Security research reports
- GitHub
- Twitter/X security feeds

7.2 Commercial Threat Feeds

- Paid threat intelligence providers
- High-quality, curated data

7.3 Internal Intelligence

- SIEM logs
- Incident reports
- SOC alerts

7.4 Dark Web & Underground Forums

- Data leaks
- Malware sales
- Credential dumps

8. Processing Threat Data

Raw threat data is often

- Unstructured
- Duplicated
- Noisy

Processing involves

- Data normalization
- De-duplication
- Enrichment (WHOIS, GeoIP, reputation)

This step prepares data for **meaningful analysis**.

9. Threat Intelligence Analysis

Analysis transforms data into intelligence.

Analysis Techniques

- Pattern recognition
- Correlation
- Trend analysis
- Behavioral analysis

Example:

- Multiple phishing campaigns using the same infrastructure → indicates a coordinated threat actor.

Analysis answers "**So what**?" instead of just "**What happened?**"

10. Threat Actor Profiling

Threat actors are categorized based on

- Motivation
- Skill level
- Resources

Common Threat Actor Types

- Cybercriminals
- Nation-state actors
- Hacktivists
- Insider threats

Understanding adversaries helps predict **future attack behavior**.

11. Indicators of Compromise (IOCs)

IOCs are observable artifacts that indicate malicious activity.

Examples:

- Malicious IP addresses
- File hashes
- Domains
- Email senders

While useful, IOCs are **short-lived**, which is why behavior-based intelligence is equally important.

12. MITRE ATT&CK & CTI Mapping

MITRE ATT&CK provides a structured way to map attacker behavior.

CTI uses ATT&CK to

- Understand attacker techniques
- Improve detection coverage
- Identify defensive gaps

This mapping improves SOC effectiveness and incident response.

13. Threat Intelligence in SOC Operations

CTI enhances SOC activities by

- Prioritizing alerts
- Enriching SIEM events
- Supporting incident investigations
- Improving threat hunting

Example:

- A login alert from a known threat actor IP is escalated faster than a generic alert.

14. Challenges

- Information overload from multiple sources
- Difficulty distinguishing noise from real threats
- Understanding attacker intent as a fresher
- Mapping intelligence to real SOC use cases

These challenges improved my analytical thinking and prioritization skills.

15. Outcomes and Learning Experience

Outcomes

- Developed a structured CTI analysis mindset
- Learned how intelligence supports SOC decisions
- Understood attacker behavior beyond tools
- Improved documentation and reporting skills

Lessons Learned

- Intelligence without context is ineffective
- Not all threats matter equally
- Quality analysis is more valuable than quantity of data
- CTI is both technical and strategic

16. Ethical Considerations

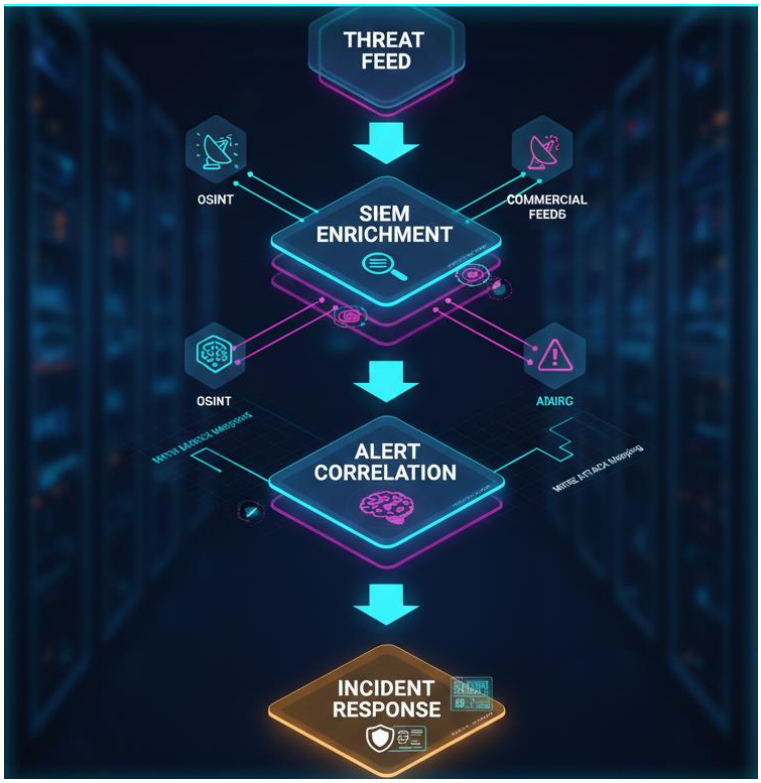
- Intelligence collection must respect legal boundaries
- No unauthorized access or exploitation
- Responsible disclosure practices followed

17. Diagrams

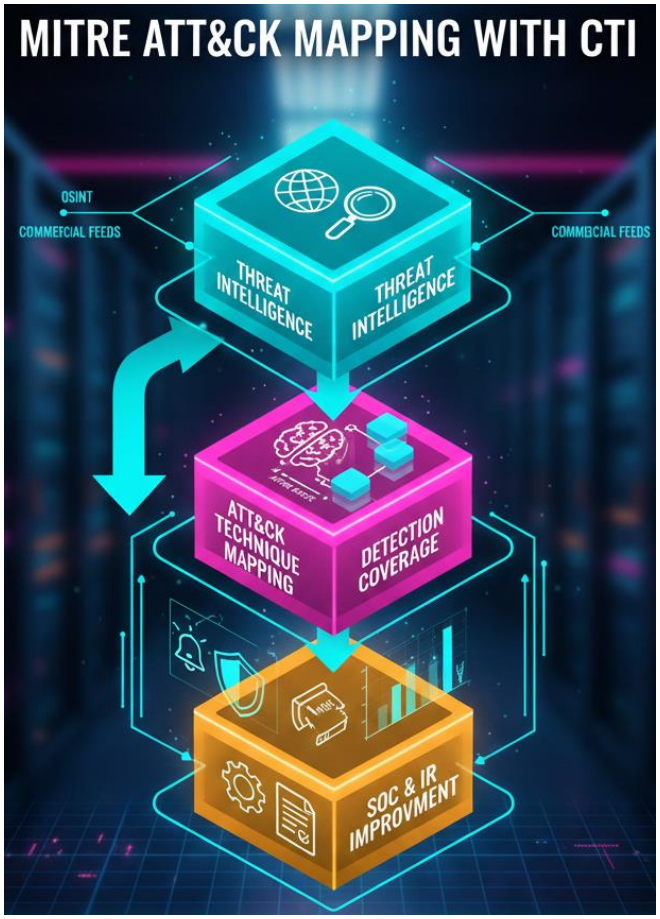
1. Threat Intelligence Lifecycle

2. Threat Intelligence Collection Sources

3. CTI Integration with SOC Workflow



4. MITRE ATT&CK Mapping with CTI



18. Conclusion

This project strengthened my understanding of **proactive cybersecurity defense**. Threat Intelligence is not about reacting to alerts—it is about **anticipating attacks before they happen**.

As a Intern, this project helped me think like.

- A SOC analyst
- A threat hunter
- A defensive strategist

This experience prepares me to contribute meaningfully in real-world security teams.