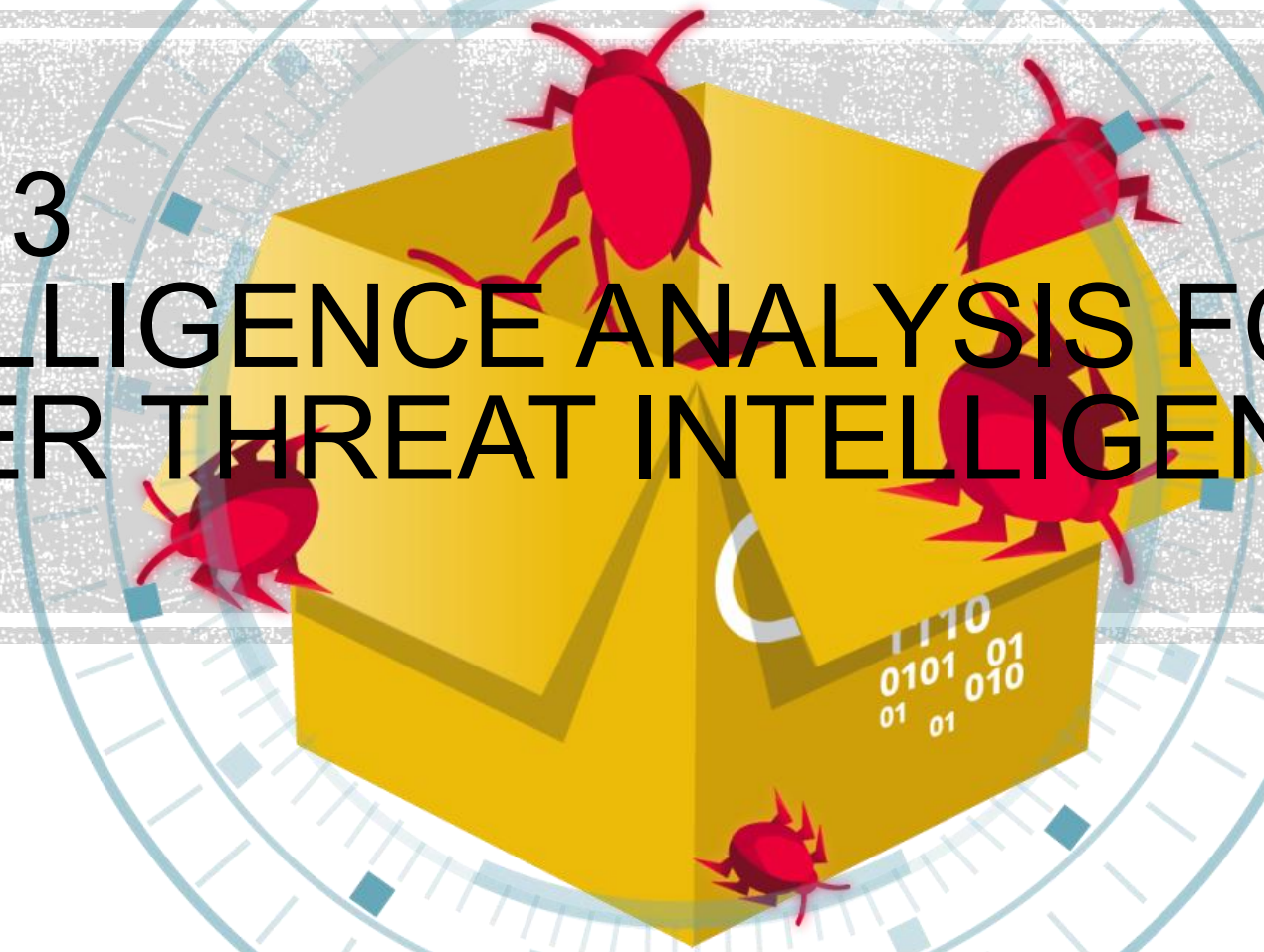
UNIT 3
INTELLIGENCE ANALYSIS FOR CYBER THREAT INTELLIGENCE (CTI)



Tejas Mhaske

Cyber Security Trainer

WHAT IS INTELLIGENCE ANALYSIS IN CTI?

- Intelligence Analysis in Cyber Threat Intelligence (CTI) is the **process of evaluating, interpreting, and contextualizing cyber threat data** to detect malicious activities and prevent security incidents.

- Intelligence analysis involves:

1. **Gathering information** from various sources, including threat feeds, network logs, and malware samples.

2. **Processing the collected data** to remove redundancies, filter noise, and categorize relevant data.

3. **Analyzing relationships between threats** to detect attack patterns, techniques, and adversary strategies.

4. **Generating actionable intelligence** to aid cybersecurity teams in mitigating threats before they cause damage.

KEY GOALS OF INTELLIGENCE ANALYSIS IN CTI:

- Identify **malware campaigns** and **threat actor tactics**.
- Detect **indicators of compromise (IOCs)** and **malicious infrastructure**.
- Provide **timely intelligence** to security teams.
- **Correlate** different threat feeds to generate **actionable insights**.
- Support **decision-making for cybersecurity operations**.

CORE COMPONENTS OF INTELLIGENCE ANALYSIS

Component	Description
Threat Actor Analysis	Identifies adversaries and their attack patterns.
Malware Behavior Analysis	Studies malware propagation and execution tactics.
Anomaly Detection	Identifies unusual network/system behaviors.
TTP Mapping	Maps threats to MITRE ATT&CK techniques.
Threat Attribution	Links cyberattacks to specific groups or nation-states.

INTELLIGENCE ANALYSIS PROCESS

Stage	Description
1. Planning & Direction	Define intelligence objectives (e.g., detect phishing campaigns).
2. Collection	Gather data from OSINT, Darknet, logs, and security feeds.
3. Processing	Normalize, clean, and structure raw data for analysis.
4. Analysis & Production	Extract patterns, detect threats, and create intelligence reports.
5. Dissemination	Share intelligence reports with stakeholders (SOC, law enforcement, etc.).
6. Feedback & Review	Improve analysis process based on operational success.

TECHNIQUES FOR DATA ANALYSIS AND VISUALIZATION

- **Why Data Analysis is Crucial in CTI?**
- Cyber threats generate **large volumes of data**. Analysts need advanced **visualization and analysis techniques** to detect attack trends.

KEY TECHNIQUES FOR THREAT DATA ANALYSIS

Technique	Use Case
Link Analysis	Identifies connections between attackers, malware, and attack infrastructure.
Heat Maps	Shows regions most affected by cyberattacks.
Timelines	Displays how threats evolve over time.
Graph-Based Analysis	Maps relationships between IOCs (e.g., IPs, domains).

INDICATORS OF COMPROMISE (IOCS) AND THEIR ANALYSIS

- **What Are IOCs?**
- IOCs are **forensic evidence** that indicates a cyberattack.
- An indicator of compromise (IOC) is evidence that someone may have breached an organization's network or endpoint.

…….. Microsoft

HOW TO IDENTIFY INDICATORS OF COMPROMISE

- When an organization is an attack target or victim, the cybercriminal will leave traces of their activity in the system and log files. The threat hunting team will gather this digital forensic data from these files and systems to determine if a security threat or data breach has occurred or is in-process.
- Identifying IOCs is a job handled almost exclusively by trained infosec professionals. Often these individuals leverage advanced technology to scan and analyze tremendous amounts of network traffic, as well as isolate suspicious activity.

WHAT TYPES OF DATA ARE CONSIDERED IOCS?

IOCs encompass diverse types of data, including:

- IP addresses
- Domain names
- URLs
- Email addresses
- Network traffic patterns
- Filenames, paths, and hash files

ANALYZING THREAT INTELLIGENCE REPORTS AND FEEDS

- **What Are Threat Intelligence Feeds?**
- These are **real-time data streams** providing information on active cyber threats.

TYPES OF THREAT INTELLIGENCE FEEDS

Type	Examples
OSINT Feeds	VirusTotal, Shodan, AlienVault OTX.
Commercial Feeds	FireEye, Recorded Future.
Community Feeds	FS-ISAC, MISP.

CTI SHARING AND COLLABORATION

- **Why is Threat Intelligence Sharing Important?**
- Enables **early warning of cyber threats**.
- Reduces **response time** against attacks.
- Encourages **cross-industry cooperation**.

METHODS OF CTI SHARING

Method	Purpose
ISACs (Information Sharing & Analysis Centers)	Sector-specific intelligence sharing (e.g., FS-ISAC for finance).
STIX/TAXII	Automated exchange of threat data.
TLP (Traffic Light Protocol)	Defines security levels for information sharing.


धन्यवाद