CYBER THREAT INTELLIGENCE

WEEK – 1

Dr. Burak Gülbay

Data | Information | Intelligence

- Sound Similar?

What is CTI?

- CTI is knowledge about threats that helps organizations defend themselves.
- It’s not just about collecting data — it’s about turning raw data into insights that allow us to make better security decisions.
- Think of it like a detective solving a case — raw clues are useless unless they are connected, analyzed, and understood in context.

Fundamentals

Data	Raw
Information	Structured
Intelligence	Actionable

Examples

01/

Data

Data is just raw facts. On its own, it may not mean much

02/

Information

Information is when that data is processed and given some context.

01/

Intelligence

Intelligence is when information is analyzed, validated, and used to support decisions.

Value Increases

- IPs, domain names, hashes, logs …
- They don’t tell us much on their own
- Noisy: not every suspicious-looking IP is truly malicious

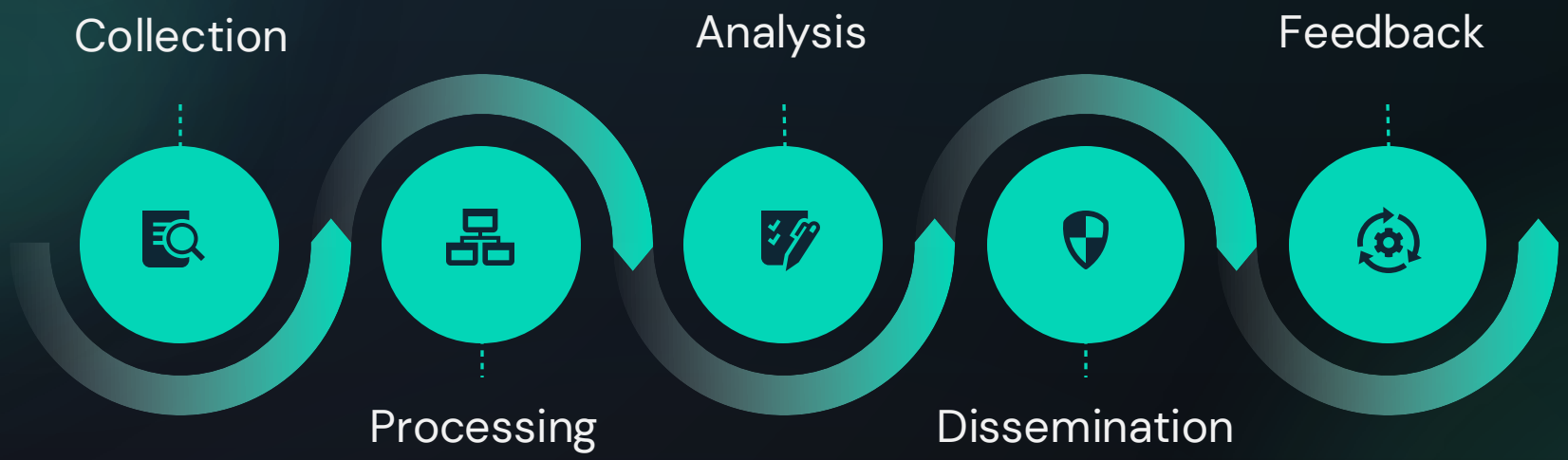
Information in Cybersecurity

- File hash linked to malware family
- Add context: data becomes information
- More meaningful — but it’s still just one piece of the puzzle.

- Correlated, analyzed, actionable: APT28 is behind phishing
- Intelligence connects the dots
- After analyzing multiple data points and information, we can assess that APT28 is running a phishing campaign against the defense sector in Turkey
- Actionable: it can guide decision-makers and defenders

Intelligence Lifecycle

Data -> Information -> Intelligence



- Start with collection of raw data,
- Process it into usable formats,
- Analyze it to extract meaning,
- Disseminate it to stakeholders,
- Finally receive feedback to improve the cycle.

This process is continuous — new data constantly feeds into updated intelligence.

Intelligence Types

Why is Distinction Important?

- The SOC might be flooded with raw data that has no clear meaning.
- Intelligence ensures the right people get the right insights at the right time.
- Without distinguishing between data, information, and intelligence, decision makers can get overwhelmed.
- Distinction indicates lifetime of intelligence.

Case Study

- An IP address shows up in logs — Data
- That IP is identified as a command-and-control server used in phishing. — Information
- The campaign is attributed to an APT group targeting the finance sector. — Intelligence

Each step adds value !

Intelligence Collection Disciplines

CTI often blends these sources to form a bigger picture

- **OSINT:** social media, blogs, forums
- **HUMINT:** informants, insider reports
- **SIGINT:** network traffic, intercepted comm.
- **TECHINT:** malware analysis, forensic data
- **GEOINT**
- **FININT**

Relation to MITRE ATT&CK

Intelligence can be mapped to attacker Tactics, Techniques and Procedures (TTPs) in ATT&CK.

For example, a malware hash can be tied to a known technique like credential dumping — which helps defenders create detections

Purpose of MITRE ATT&CK:

- Standardized Knowledge Base of Threat Behaviors
- Threat Modeling and Simulation
- Gap Analysis and Defense Prioritization
- Incident Response and Threat Hunting
- Industry Collaboration and Knowledge Sharing

Common Pitfalls

THINK ABOUT FOLLOWINGS

01/

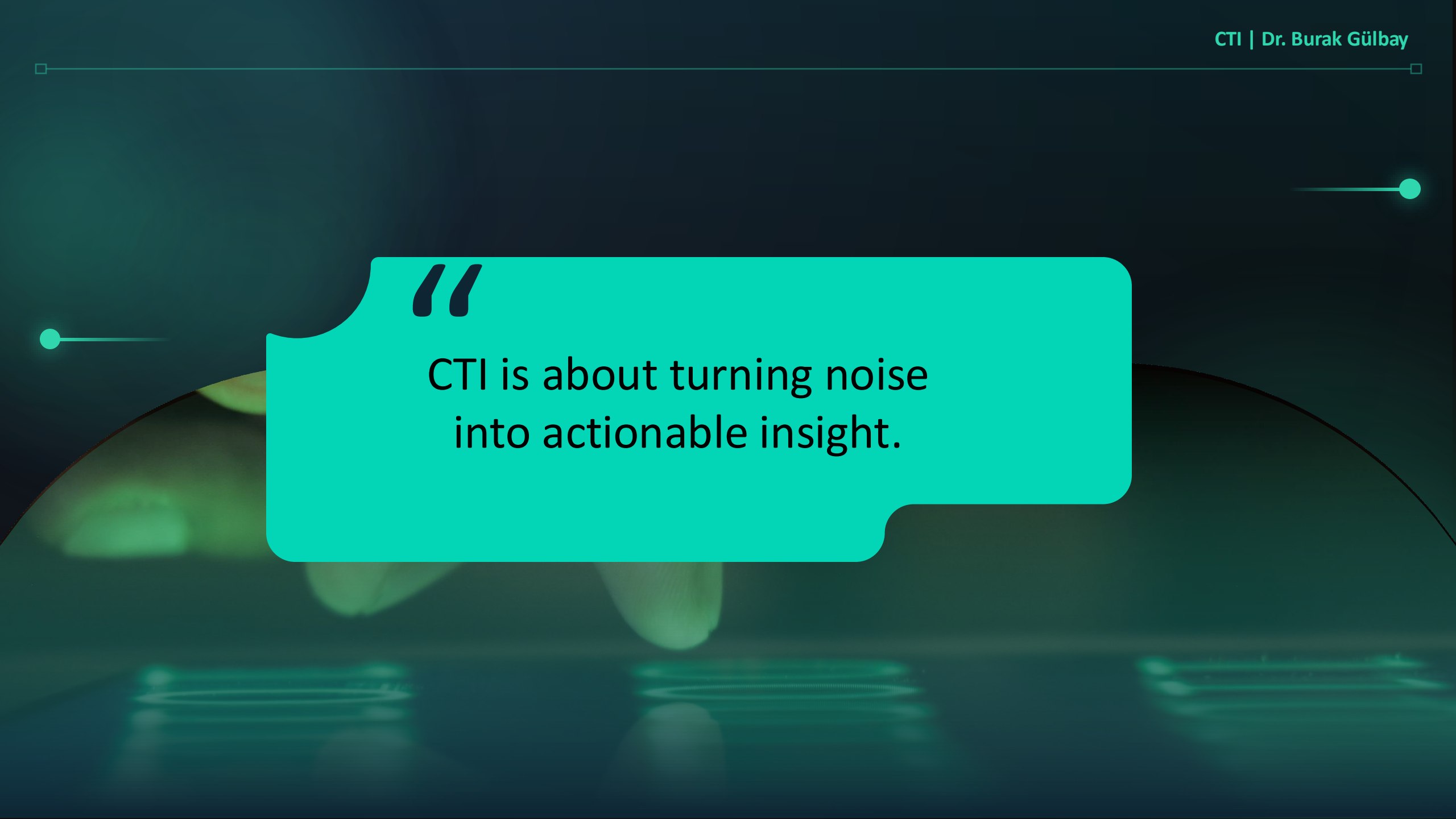
A common mistake is treating raw data as intelligence.

02/

Over-reliance on automated threat feeds without human analysis.

03/

Intelligence is useless if it’s not validated and put into context.



> CTI is about turning noise into actionable insight.