- Filename: eccouncil-ceh31250-v11-1-13-1-cyber-threat-intelligence.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Cyber Threat Intelligence

==

Cyber Threat Intelligence

Objectives:

- Define CTI
- Describe how CTI is used to engage in threat modeling
- List and define the 4 types of CTI

- How do we define CTI?
    - The gathering, processing, and analysis of data about threats.
        - Purpose of understanding
            - Motives
            - Targets
            - Attack Behaviors
        - Aids defenders
            - Faster
            - Better equipped to withstand attacks
            - More informed defensive strategies
            - Be proactive instead of reactive
            - Possibly reveal unknown threats
- What are the different types of CTI?
    - Strategic
    - Operational
    - Tactical
    - Technical
- Why do we break CTI down into these categories?
    - To speak to different audiences
        - High-level
            - Managers
                - Business Strategy
                    - Strategic CTI
                        - How do we deal with the likely threats to our organization?
                        - Sources:
                            - OSINT
                            - CTI Vendors
                    - Operational CTI
                        - Specific attacks against your organization
                            - APT reports

- I assume that there is 'Low-level' then?
    - Yes
        - Low-level
            - Technicians/Engineers
                - Operational deployment strategies
                    - Tactical CTI
                        - Sources:
                            - Malware analysis
                            - IH&R reports
                            - APT reports
                    - Technical CTI
                        - Very specific information
                            - More ATOMIC information
                                - Tactical = Phishing email
                                - Technical = Malicious link in phishing email