- Filename: eccouncil-ceh31250-v12-1-16-1-mitre-att&ck-framework.md
- Show Name: CEHv12 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Basic Cybersecurity Concepts

==

Mitre ATT&CK Framework

Objectives:

---

1. What is the Mitre ATT&CK Framework

- https://attack.mitre.org
- Knowledge Base

    - Consists of...

        - Matrices

    - Enterprize
    - Mobile
    - ICS

        - Adversarial tactics and techniques

    - Derived from real-world experience
    - Used by cybersecurity professionals to prepare their systems for common attack methods

2. How does one use ATT&CK Matrices?

- Choose your matrix
- Layout

    - Tactics Columns

        - Techniques(number of sub-techniques)

3. Explain these tactics, techniques, and sub-techniques

- **Tactics**

    - WHY an adversary uses a specific technique/sub-technique

- **Techniques**

    - HOW and adversary achieves a tactical goal (what ACTION do they take?)

- **Sub-Techniques**

    - More specific techniques

4. Now, how do we use the ATT&CK framework?

- We can now do things like Threat Modeling

    - ATT&CK Navigator