MITRE ATT&CK®

- Is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Is used as a foundation for the development of specific threat models and methodologies.
- Attack STIX contains several csvs, organized in folders following the next structure:

```
├─ enterprise-attack ····················· Collection folder for MITRE
ATT&CK Enterprise
│   ├─ enterprise-attack.json ·············· Most recent Enterprise
release
│   ├─ enterprise-attack-9.0.json ·········· Enterprise ATT&CK v9.0
collection
│   └─ [other releases of Enterprise ATT&CK]
├─ mobile-attack
│   └─ [Mobile ATT&CK releases]
├─ ics-attack
│   └─ [ATT&CK for ICS releases]
├─ index.json ···························· Collection index JSON
└─ index.md ····························  Collection index markdown
```

- Focusing on enterprise-attack, it contains more than 1630 elements with:
  type [16307]
  id [16307]
  spec_version [16307]
  x_mitre_attack_spec_version [16307]
  created [16307]
  x_mitre_version [16306]
  modified [16306]
  x_mitre_domains [16306]
  created_by_ref [16172]
  object_marking_refs [16172]
  x_mitre_modified_by_ref [16170]
  target_ref [14467]
  source_ref [14467]
  relationship_type [14467]
  description [13689]
  external_references [12802
  And other information present in less than ~10% of the elements