**MITRE ATT&CK FRAMEWORK**

MITRE ATT&CK is an abbreviation for Adversarial Tactics, Techniques and Common Knowledge.

It is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This framework is used in Cyber Threat Intelligence Analysis. CTI Analysis is taking existing intelligence like TTPs(Tactic, Technique, Procedure), malware hashes and using human intelligence to harden cyber defenses.

MITRE developed a free, open-source tool CRITS (Collaborative Research into Threats). This tool helps with CTI analysis by collecting and associating attack artifacts with stages of cyber attack lifecycle, conducting malware reverse engineering and finally connecting all this together to prioritize defenses and react to incidents.

**Tactic** – Technical goals the adversary wants to achieve.

**Technique** – How these goals are achieved.

**Procedure** – Implementation of the techniques.