Muskan Shaikh

MITRE ATT&CK FRAMEWORK

WHAT IS MITRE ATT$CK FRAMEWORK ?

- Mitre is a non-profitable organization which work with the companies to help them proteck themselves and provide deep insight into attacker behaviour.
- Mitre attack helps to identify most of the attacks and mitigate them.
- It was created by the Mitre Corporaton and released in 2013.
- Attacks stands for Adversarial, Tactics, Techniques, and Common Knowledge.

ATT$CKS DESCRIPTION OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) PROVIDES DEEP INSIGHT INTO ATTACKER BEHAVIOUR.

- ADVERSARIAL TACTICS : Describe their goals, like getting inside your network or stealing credentials.
- TECHNIQUES : Show how they do it, Spear phishing
- Procedures/ Common knowledge : Highly detailed examples of the tools and actions of specific attacker groups.

ATT$CK MATRIX