MITRE ATT&CK

Inhaltsverzeichnis

MITRE ATT&CK ist eine Wissensbasis zu Taktiken und Techniken von Angreifern. Teams nutzen sie, um Detection, Purple-Teaming und Abwehrlücken entlang realer Angriffsmuster zu strukturieren.

1 Funktionsweise

Angriffe werden in Taktiken (Ziele) und Techniken (Vorgehen) zerlegt. Security-Controls und Use Cases lassen sich diesen Bausteinen zuordnen und auf Abdeckung prüfen.

- **Tactics:** z. B. Persistence, Lateral Movement
- **Techniques/Sub-Techniques:** konkrete Methoden
- **Matrices:** Enterprise, Cloud, ICS u. a.

2 Typische Einsatzbereiche

- Detection Engineering und SIEM-/EDR-Use-Cases
- Gap-Analysen der Abwehr
- Red-/Purple-Team-Planung

3 Wichtige Hinweise

- ATT&CK ist kein Compliance-Checkbox-Katalog.
- Priorisierung nach eigenem Bedrohungsbild nötig.
- Technik-IDs in Alerts erleichtern die Kommunikation.

4 Fazit

MITRE ATT&CK schafft eine gemeinsame Sprache für Angriffsverhalten – unverzichtbar, um Detection und Abwehr systematisch statt zufällig auszubauen.