AYI NEDJIMI Consultants

MITRE ATT&CK 2026 : Framework TTPs, Tactiques et Techniques

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3576 mots • 130 vues •

> Le framework MITRE ATT&CK est la knowledge base de référence des tactiques, techniques et procédures adversaires. Guide complet 2026 : matrices Enterprise/ Mobile/ICS/Cloud, Groups, Software, Navigator, Workbench, intégrations SIEM/EDR et use cases Red, Blue et Purple Team.

Le framework **MITRE ATT&CK** (Adversarial Tactics, Techniques and Common Knowledge) est la knowledge base de référence mondiale documentant les tactiques, techniques et procédures (TTPs) employées par les adversaires lors de cyberattaques réelles. Maintenu depuis 2013 par la **MITRE Corporation**, org
non lucratif financée par le gouvernement fédéral ar

structure la connaissance offensive selon une matrice où chaque colonne représente une tactique (objectif adverse) et chaque cellule une technique observée dans la nature. La version v15+ couvre en 2026 plus de **14 tactiques Enterprise**, **200+ techniques** et **400+ sous-techniques**, complétées par des matrices spécialisées Mobile, ICS, Cloud et Containers. ATT&CK est devenu le langage commun des équipes Red Team, Blue Team, SOC, threat hunters, éditeurs SIEM/EDR et CTI : il permet de cartographier la couverture défensive, prioriser les détections, simuler des adversaires connus (APT28, Lazarus, FIN7) et mesurer la maturité d'un programme de cybersécurité. Gratuit, open source et lié au format STIX/TAXII, ATT&CK est aujourd'hui intégré nativement dans Microsoft Sentinel, CrowdStrike Falcon, Splunk, Elastic et Wazuh.

À RETENIR

L'essentiel à retenir

MITRE ATT&CK est une knowledge base ouverte recensant les TTPs adversaires observés dans des intrusions réelles depuis 2013.

La matrice Enterprise compte 14 tactiques (de Reconnaissance à Impact) et plus de 200 techniques identifiées par des codes TXXXX.

Les Groups (G####) et Software (S####) cartographient les acteurs malveillants et leurs outils.

Réponse sous 24h

Devis gratuit →