MEMAHAMI MITRE ATT&CK: PANDUAN KERANGKA KEAMANAN SIBER

APA ITU WEBSITE & FRAMEWORK MITRE ATT&CK?

- DATABASE CARA HACKER MENYERANG SISTEM
- DARI TEKNIK MASUK SAMPAI MENCURI DATA

MITRE ATT&CK = PETA CARA HACKER BEKERJA

Datarah base pengetahuan pubk untuk modeling, memetetansi, dan monnitoring cyber thragan berdasarkan perilakul realli attacker real.

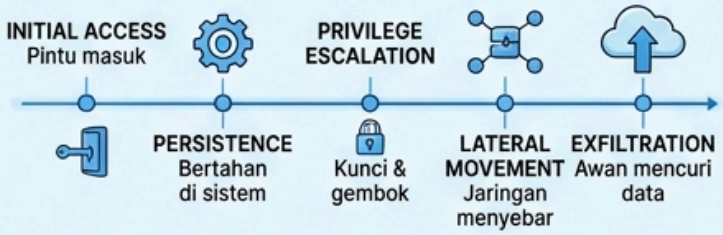
ARTI NAMA ATT&CK

- Adversarial Tactics → TUJUAN SERANGAN
- Techniques → CARA MENYERANG
- & Common Knowledge → PENGETAHUAN SERANGAN NYATA

APA ISI WEBSITENYA?

- TAHAPAN SERANGAN HACKER
- TEKNIK YANG DIGUNAKAN (RATUSAN)
- CONTOH MALWARE / THREAT ACTOR
- CARA DETEKSI & MITIGASI

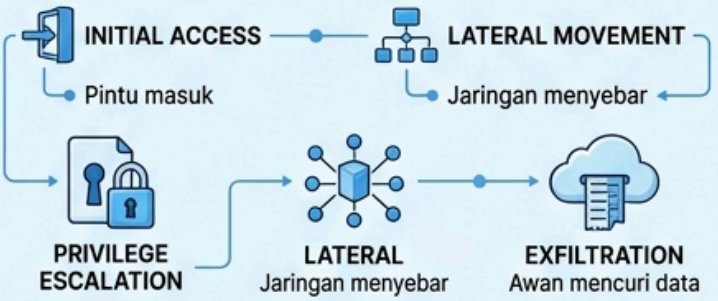
CONTOH TAHAPAN SERANGAN (MATRIX)



UNTUK APA DIPAKAI?

MEMBANTU ORGANISASI MEMAHAMI TTP (TACTICS, TECHNIQUES, PROCEDURES) PENYERANG

CONTOH TAHAPAN SERANGAN (MATRIX)



UNTUK APA DIPAKAI?

MEMBANTU ORGANISASI MEMAHAMI TTP (TACTICS, TECHNIQUES, PROCEDURES) PENYERANG

ANALOGI SEDERHANA

KEAMANAN SIBER	VS	MITRE ATT&CK
= PERANG Soldiers defending		= BUKU STRATEGI MUSUH Hacker tactics handbook

KENAPA PENTING BANGET (SERING LIHAT DI SOC)

- Banyak SIEM mapping ke MITRE
- Digunakan di laporan insiden
- Dipakai BSSN & industri
- Standar global threat intel