



# MEMAHAMI MITRE ATT&CK: PANDUAN KERANGKA KEAMANAN SIBER

## APA ITU WEBSITE & FRAMEWORK MITRE ATT&CK?



### MITRE ATT&CK = PETA CARA HACKER BEKERJA

Datarah base pengetahuan publik untuk modeling, memetatesi, dan monitoring cyber thragan berdasarkan perilaku realli attacker real.

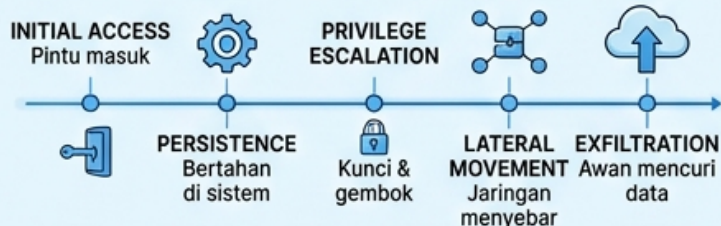
## ARTI NAMA ATT&CK



## APA ISI WEBSITENYA?

- ✓ 1 2 3 TAHAPAN SERANGAN HACKER
- ✓ TEKNIK YANG DIGUNAKAN (RATUSAN)
- ✓ CONTOH MALWARE / THREAT ACTOR
- ✓ CARA DETEKSI & MITIGASI

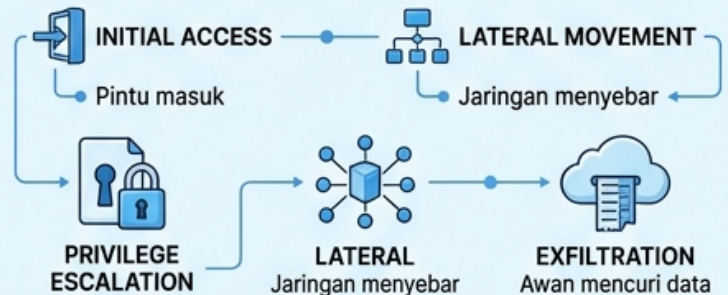
## CONTOH TAHAPAN SERANGAN (MATRIX)



## UNTUK APA DIPAKAI?



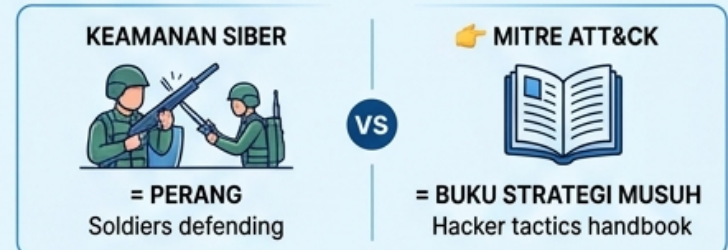
## CONTOH TAHAPAN SERANGAN (MATRIX)



## UNTUK APA DIPAKAI?



## ANALOGI SEDERHANA



## KENAPA PENTING BANGET (SERING LIHAT DI SOC)

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



## DISKOMINFOS PROVINSI BALI

### PROGRAM LITERASI KESADARAN KEAMANAN SIBER

Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?  
Ayo berlangganan KABAR LENTERA (GRATIS !) di <https://balikom.info/kabarlentera>



**SECURITY**  
IS INCOMPLETE WITHOUT U  
**#JagaRuangSiber**



**SAYA NETIZEN CERDAS**

[DISKOMINFOS.BALIPROV.GO.ID](https://diskominfo.baliprov.go.id)

[diskominfo.bali](https://diskominfo.bali)

[diskominfo\\_bali](https://diskominfo.bali)

[lenterasiber](https://lenterasiber)

[balikom.info/link/lenterasiber](https://balikom.info/link/lenterasiber)

TLP: CLEAR



Dokumen ini telah ditandatangani secara elektronik (TTE).  
Scan/Klik QR Code untuk informasi TTE.  
Upload file pada <https://tte.komdigi.go.id/verifyPDF> untuk cek keaslian file.

