

RED TEAM VS BLUE TEAM

Dua Peran Penting Keamanan Siber

Dalam keamanan siber, terdapat dua peran tim yang menyerang untuk menguji (Red Team) dan tim yang melindungi sistem (Blue Team). Tujuannya sama-sama untuk melindungi ruang siber instansi tetap aman.

● RED TEAM

TIM PENYERANG (Hacker)

- Mensimulasikan serangan seperti hacker.
- Mereka mencari celah sebelum penjahat siber menemukannya.
- Tujuannya untuk menemukan kelemahan suatu sistem.

Contoh Aktivitas:

- Pentest website
- Phishing simulation
- Exploit kerentanan
- Social engineering
- Uji keamanan jaringan



Vs

● BLUE TEAM

TIM PERTAHANAN (Defender)

- Melakukan deteksi dan menghentikan serangan.
- Mereka menjaga sistem tetap aman setiap hari.
- Tujuannya untuk melindungi dan memulihkan suatu sistem dari serangan siber.

Contoh Aktivitas:

- Monitoring log (SOC)
- Incident response
- Hardening server
- Patch update
- Analisis malware



Kenapa Kedua Team ini Berperan Penting?

- Tanpa Red Team → celah serangan siber tidak terlihat.
- Tanpa Blue Team → serangan siber tidak tertangani.
- Adanya Purple Team → menghubungkan hacker dan defender.
- Saling berbagi hasil serangan → memperkuat keamanan siber.



DISKOMINFOS PROVINSI BALI

PROGRAM LITERASI KESADARAN KEAMANAN SIBER

Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?

Ayo berlangganan KABAR LENTERA (GRATIS !) di <https://baliikom.info/kabarlentera>



SECURITY
IS INCOMPLETE WITHOUT U
#JagaRuangSiber



SAYA NETIZEN CERDAS

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

[f diskominfofbali](https://facebook.com/diskominfofbali)

[i diskominfo_bali](https://instagram.com/diskominfo_bali)

[lenterasiber](https://twitter.com/lenterasiber)

baliikom.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.

