RED TEAM

Red Teaming and the Adversarial Mindset

redteams.net

A Red Team views a problem from an adversary perspective.

A good Red Team is a "*thinking enemy*", challenging planning assumptions and helping leaders to understand and address the risks.

Red Teams test the entire security posture of the organization:

Physical, Digital and Social.

Adversaries don’t play by the same rules as the good guys. In fact they don’t have rules at all.

They adapt.

Think of a hollow cube: you have the 6 external sides to check, yet you can't forget the 6 internal sides.

Go beyond the visible, the obvious. Check the extra things that no one has bothered to test before.

Remember: the reverse side has also a reverse side. Never assume and always verify.

Adversaries *can* and *will* exploit any and all known attack vectors. They will also create new ones.

Attackers get very creative. Especially when they are motivated.

"One thing a person cannot do, no matter how rigorous his analysis or heroic his imagination, is to draw up a list of things that would never occur to him."

Thomas Shelling

Systems will be compromised.
Perimeters will be breached.

You can’t just throw money at the problem.

If everything seems to be going well, you have obviously overlooked something.

Rule 29:

If you're happy with your security, so are the bad guys.

Defenders often are so focused on the systems they want to protect, they forget one very basic truth…

Attackers are extremely good

at exploiting the human factor.

The modern organizations are too complex for any individual or group to thoroughly understand how it can be compromised.

To become the enemy,
see yourself as the enemy
of my enemy.

Musashi

Security plans and strategy sometimes are governed by what worked in the past and not on the dynamic world of the attackers.

Unless trained to think differently, security professionals tend to have a plan of action based on the past and on lists that other security professionals created.

The adversary doesn’t care about the past.

You have to ask the right questions. The questions that no one wants to answer...

Remember:
When in doubt, Red Team it.