
# The secrets of effective red teaming

Chathura Abeydeera[1]
[1]*eSecure Pty Ltd*

A red team is a collective of different specialists who perform goal-based simulated adversarial activities. The purpose of conducting such assessment is to demonstrate the tactics of real-world attackers in the wild utilising to compromise the business process of the organisations.

An effective red team exercise will test the organisation's defences, attack detection and its incident response capabilities. On occasion this goal-based attack stratagem may be intelligence lead, or hybrid approach with intelligence fused with different adversarial modelling.

Putting together a red team requires a "malicious mindset", technical talent and vision to drive the program to success. Building a high impact red team will increase the organisation's security posture by performing holistic testing and emulating real world threat actors.

Securing red team infrastructure is as equally important as achieving the nominated goals. Often irresponsible red teams get hunted by internet vigilantes, results of this can be vary from loss of reputation to complete compromise of the organisation.

This presentation will be focusing on providing insights of how a read team works, how to make a good red team "great" by making outstanding playbooks and how not to get owned by the avengers. Organisations will get hacked, will get breached. Prepare!