

Red, Blue, and Purple Teams: Running the Fight on Purpose

Sat, Aug 15, 2:00 PM EDT · <https://scottslab.io/posts/red-blue-and-purple-teams>

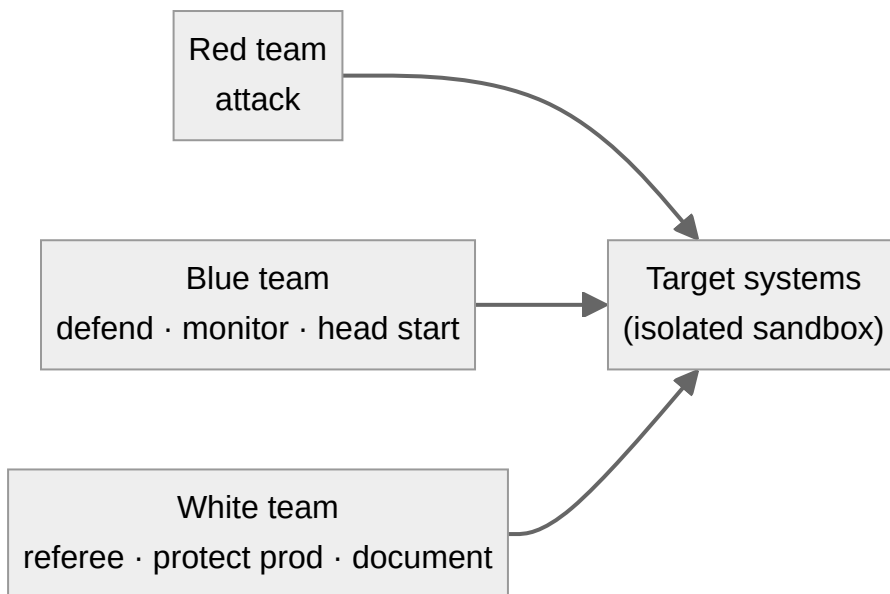


TL;DR

A security exercise splits into teams: red attacks, blue defends (usually with a head start), and a white team referees to keep it out of production and write up the lessons. Purple teaming is the part that actually makes you better: red and blue sharing findings afterward so the attacks teach the defenses. Capture the Flag gives red concrete objectives scored against blue's prevention, and all of it runs in an isolated sandbox, never on live systems.

The colored teams are just roles in a staged fight, and knowing them keeps the point in view: you're not trying to win, you're trying to learn where you'd lose.

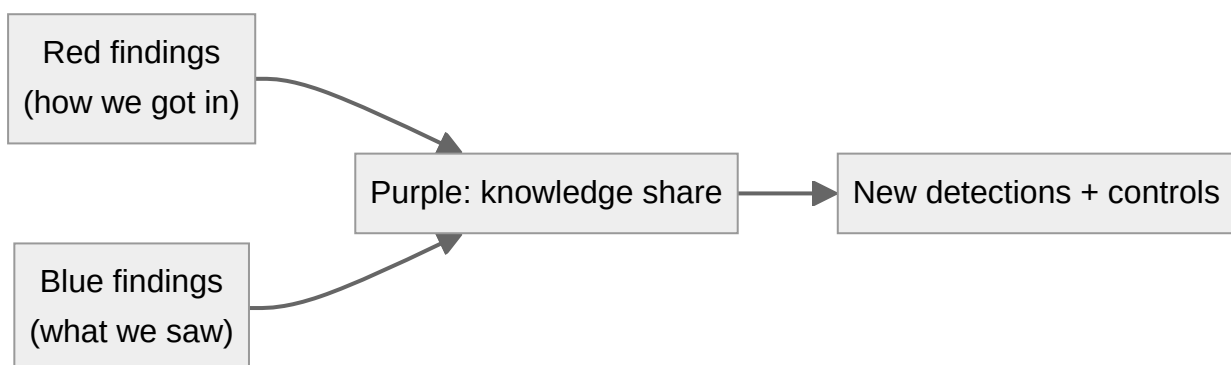
Red team is offense: they attempt to compromise systems, playing the adversary as realistically as the rules allow. Blue team is defense: securing, monitoring, and responding. They usually get a head start, because the exercise is testing whether prepared defenders can hold, not whether they can be ambushed cold. The tension between the two is the whole product: red finds the gaps, blue finds out whether they can see and stop what red is doing.



Red, Blue, and Purple Teams: Running the Fight on Purpose

There's a third team people forget: the white team, the observers and referees. They set the boundaries, make sure the exercise doesn't spill into production and cause a real outage, adjudicate disputes, and, most importantly, document the lessons learned. Without a white team, an exercise either descends into chaos or quietly damages something real, and either way nobody writes down what happened.

The color that matters most is purple. Purple teaming isn't a separate squad so much as what happens after the whistle: red and blue sit down together and combine findings, so every attack red pulled off becomes a detection or control blue builds next. An exercise where red "wins" and walks away taught you nothing; the value is entirely in the debrief where offense explains exactly how, and defense turns that into coverage. A common format is Capture the Flag: red pursues specific objectives, the flags, scored against blue's ability to prevent them. That keeps the whole thing concrete and measurable.



Red, Blue, and Purple Teams: Running the Fight on Purpose

One rule runs under all of it: these exercises happen in isolated sandbox environments, not on production systems. You're deliberately trying to break things and deploy real attack techniques;

doing that against live infrastructure trades a learning exercise for a self-inflicted incident. Build the range, run the fight there, and bring the lessons back.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — <https://scottslab.io/posts/red-blue-and-purple-teams>