**Red, Blue, and Purple Teams**

There is some confusion about the definitions of Red, Blue, and Purple teams within Information Security. Here are my definitions and concepts associated with them.

**Definitions**

**Red Teams**: are internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible. The practice is similar, but not identical to, [Penetration Testing](https://danielmiessler.com/study/vulnerability-assessment-penetration-test/), and involves the pursuit of one or more objectives—usually executed as a campaign.

**Blue Teams** refer to the internal security team that defends against both real attackers and Red Teams. Blue Teams should be distinguished from standard security teams in most organizations, as most security operations teams do not have a mentality of constant vigilance against attack, which is the mission and perspective of a true Blue Team.

**Purple Teams** exist to ensure and maximize the effectiveness of the Red and Blue teams. They do this by integrating the defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team into a single narrative that maximizes both. Ideally Purple shouldn’t be a team at all, but rather a permanent dynamic between Red and Blue.

**Red Teams**

Red Teams are most often confused with [Penetration Testers](https://danielmiessler.com/blog/the-difference-between-a-penetration-test-and-a-red-team-engagement/), but while they have tremendous overlap in skills and function, they are not the same.

Red Teams have [a number of attributes](https://danielmiessler.com/blog/five-attributes-effective-corporate-red-team/) that separate them from other offensive security teams. Most important among those are:

* Emulation of the TTPs used by adversaries the target is likely to face, e.g., using similar tools, exploits, pivoting methodologies, and goals as a given [threat actor](https://danielmiessler.com/blog/explaining-threats-threat-actors-vulnerabilities-and-risk-using-a-real-world-scenario/).
* Campaign-based testing that runs for an extended period of time, e.g., multiple weeks or months of emulating the same attacker.

If a security team uses standard pentesting tools, runs their testing for only one to two weeks, and is trying to accomplish a standard set of goals—such as pivoting to the internal network, or stealing data, or getting domain admin—then that’s a Penetration Test and not a Red Team engagement. Red Team engagements use a tailored set of TTPs and goals over a prolonged period of time.

It is of course possible to create a Red Team campaign that uses the best-of-the-best TTPs known to the Red Team, which uses a combination of common pentesting tools, techniques, and goals, and to run that as a campaign (modeling a Pentester adversary), but I think the purest form of a Red Team campaign emulates a specific threat actor’s TTPs—which won’t necessarily be the same as if the Red Team were attacking itself.

**Blue Teams**

The goal here is not gatekeeping, but rather the encouragement of curiosity and a proactive mentality.

Blue Teams are the proactive defenders of a company from a cybersecurity standpoint.

There are a number of defense-oriented InfoSec tasks that are not widely considered to be Blue-Team-worthy, e.g., a tier-1 SOC analyst who has no training or interest in offensive techniques, no curiosity regarding the interface they’re looking at, and no creativity in following up on any potential alerts.

All Blue Teams are defenders, but not all defenders are part of a Blue Team.

What makes a Blue Team vs. just doing defensive things is the mentality. Here’s how I make the distinction: Blue Teams / Blue Teamers have and use:

A proactive vs. reactive mindset

Endless curiosity regarding things that are out of the ordinary

Continuous improvement in detection and response

It’s not about whether someone is a self-taught tier-1 SOC analyst or some hotshot former Red Teamer from Carnegie Mellon. It’s about curiosity and a desire to constantly improve.

**Purple Teams**

Purple is a cooperative mindset between attackers and defenders working on the same side. As such, it should be thought of as a function rather than a dedicated team.

The true purpose of a Red Team is to find ways to improve the Blue Team, so Purple Teams should not be needed in organizations where the Red Team / Blue Team interaction is healthy and functioning properly.

The best uses of the term that I’ve seen are where any group not familiar with offensive techniques wants to learn about how attackers think. That could be an incident response group, a detection group, a developer group—whatever. If the good guys are trying to learn from whitehat hackers, that can be considered a Purple Team exercise.