RED, BLUE, & PURPLE TEAMS OF CYBERSECURITY

Balbix®

Cybersecurity is a Team Sport

Red team vs. blue team exercises are an innovative security strategy that simulates real-life cyberattacks in order to locate weaknesses, improve information security, and maximize the effectiveness of defenses.

This adversarial team effort provides a realistic assessment of the organization’s security posture by leveraging the expertise of specialized teams with specific goals, heightened risk awareness, sharpened skills, and a continuous improvement mindset.

The Players

Red Teams

- Offensive security professionals
- Expert at attacking systems and breaking into defenses
- Responsible for testing the effectiveness of security programs by emulating the tools and techniques of likely hackers

Blue Teams

- Defensive security specialists
- Expert at maintaining internal network defenses against all cyber-attacks and threats
- Responsible for defending against both real attackers and red teams as they maintain a constant vigilance against attacks

Balbix®

Let the Games Begin

War gaming the security infrastructure is a strategic form of proactive defense used by government agencies, the corporate world, and beyond.

Although the word "game" has a playful connotation, red team/blue team engagements are SERIOUS BUSINESS.

These cybersecurity war games pit red teams, whose job it is to attack, exploit, and circumvent an organization's security controls, against blue teams, who are charged with holding the fort by detecting, preventing, and defeating attacks.

As red teams simulate attacks against blue teams to test the effectiveness of the network's security, these exercises can help strengthen defenses against both current and evolving threats.

Join the Red

- Know how to think like a hacker
- Test the effectiveness of organization's security program
- Emulate the tools, techniques, and processes used by likely adversaries
- Runs tests over a prolonged period of time to find vulnerabilities
- Provide a complete audit of testing results

Go into the Blue

- Know how to defend against both real attackers and red teams
- Proactively protect the organization against cyber-attacks
- Maintain a constant vigilance over the security posture
- Adjust security posture based on red team insights
- Continuously improve detection and response

Balbix®

By the Numbers

60% of the companies surveyed conduct such exercises

24%
do it monthly

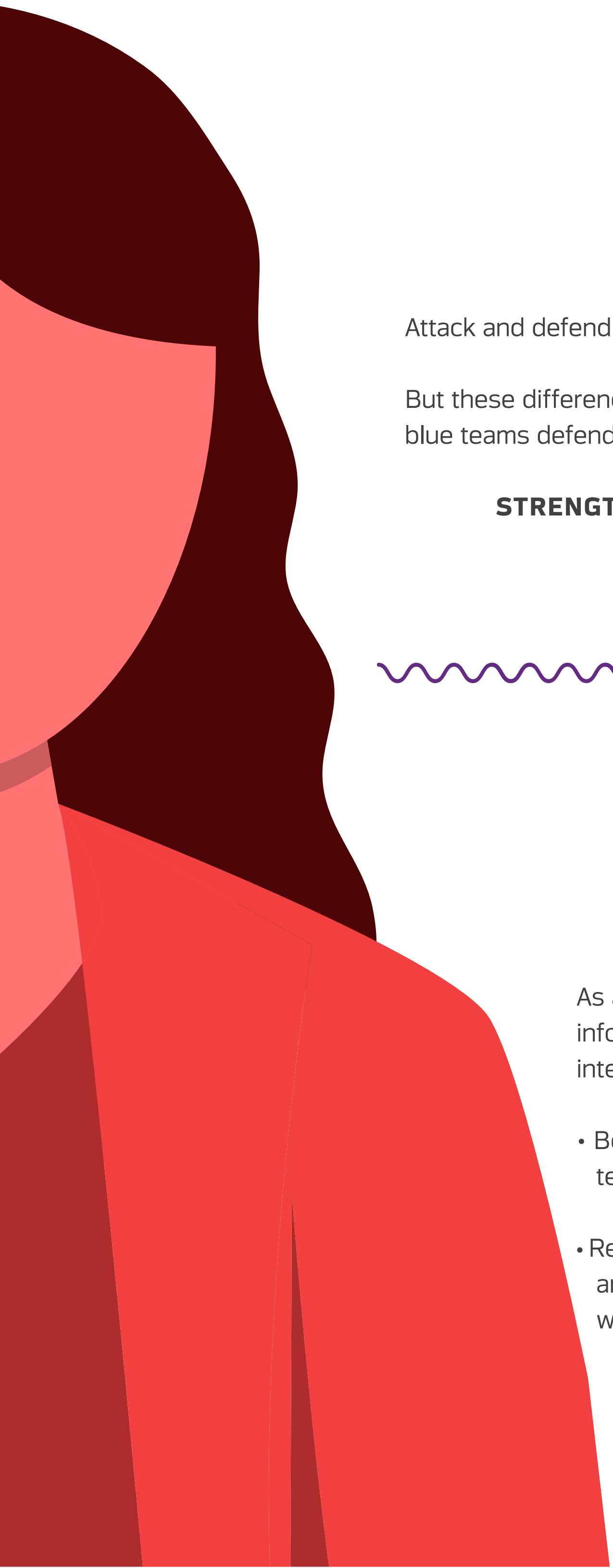
12%
do it quarterly

11%
do it bi-annually

13%
13% do it annually

3 in 4
IT security professionals say their companies have increased security infrastructure investment as a result of red and blue team testing

1 in 5
say these budget changes have been significant



An Eye on the Prize

Attack and defend, red and blue teams could not be more opposite in their tactics and behaviors.

But these differences are precisely what make them a part of an effective whole. As red teams attack and blue teams defend, their shared primary goal is simple.

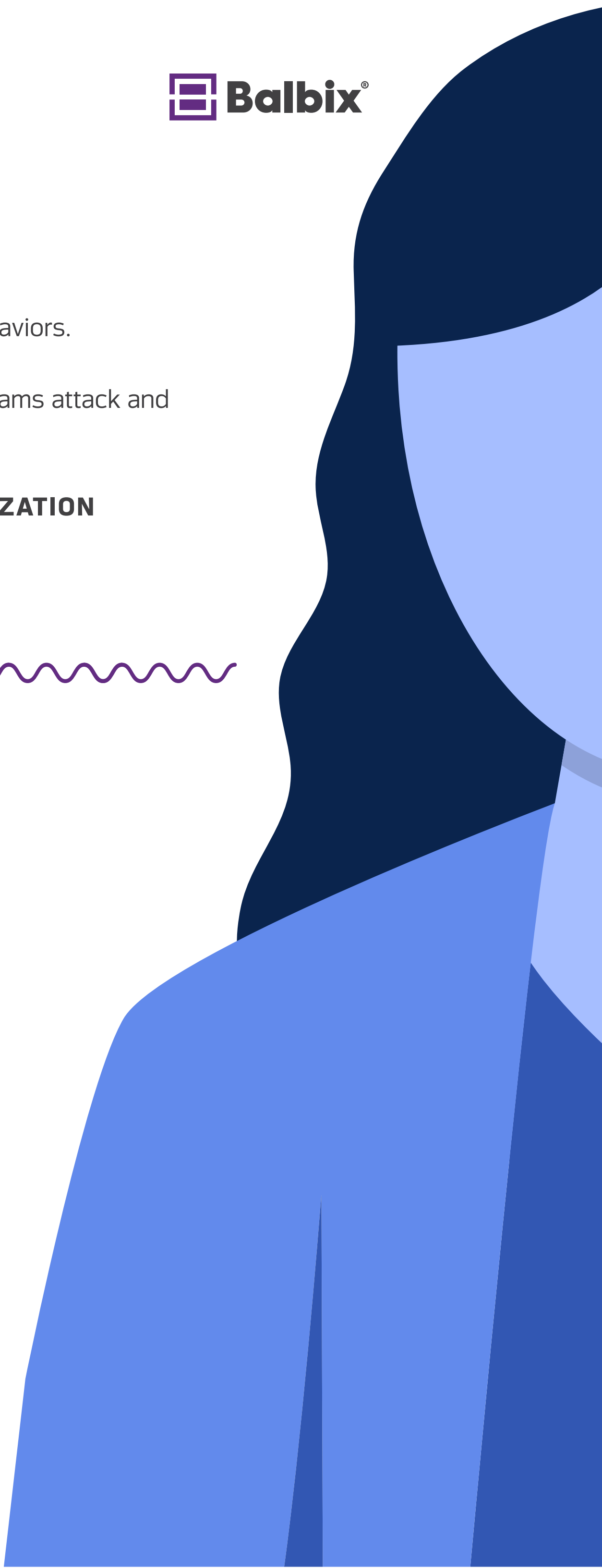
STRENGTHEN THE OVERALL CYBERSECURITY POSTURE OF THE ORGANIZATION

Creating a Closed-Loop System

As a red team member, there's no point in winning if you're not sharing that information with the blue team. There needs to be a continuous dialog and integration between the two teams.

- Both teams need to work together to provide a complete audit of every test that was performed, what succeeded, what didn't, and why.
- Red teams will provide detailed logs of all the operations they performed, and blue teams will completely document all the corrective actions that were taken to address the issues that were found during testing.

THIS IS WHERE THE PURPLE TEAM COMES IN.

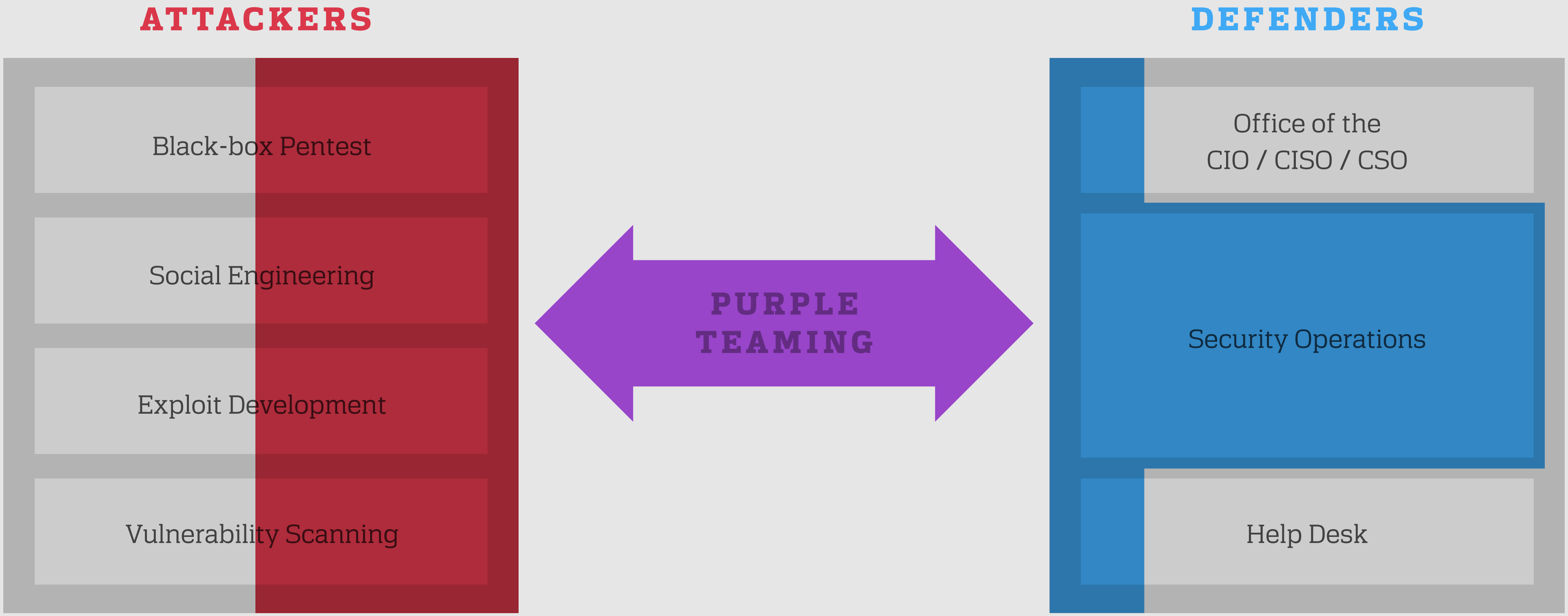


Purple Teams

- Bring both red and blue teams together.
- May be a separate internal or external team or just management/security infrastructure.
- Integrate defensive tactics and controls from the blue team with threats and vulnerabilities found by the red team into a single narrative that maximizes the overall effectiveness of both.
- Ensure that red and blue teams are sharing insights and creating a strong feedback loop that drives continuous improvement.

In an ideal world, purple isn't a separate team at all, but rather a permanent dynamic between red and blue teams within the organization.

Bridging Blue and Red Teams



ATTACKERS

Black-box Pentest

Social Engineering

Exploit Development

Vulnerability Scanning

PURPLE TEAMING

DEFENDERS

Office of the CIO / CISO / CSO

Security Operations

Help Desk

Balbix®

AI-Powered Cybersecurity Posture Transformation

References

https://danielmiessler.com/study/red-blue-purple-teams/

https://purplesec.us/red-team-vs-blue-team-cyber-security/

https://blog.eccouncil.org/red-team-vs-blue-team/

https://www.darkreading.com/endpoint/68--of-companies-say-red-teaming-beats-blue-teaming/d/d-id/1335529

http://www.circleid.com/posts/20161130_the_purple_team_pentest/