RED TEAM

Think Like an Attacker

Objective:
Simulate real-world cyberattacks to uncover exploitable weaknesses.

Key Activities:

- Penetration Testing
- Social Engineering
- Adversary Simulation
- Exploit Validation

Measures: How easily can attackers compromise us?

BLUE TEAM

Defend Against Threats

Objective:
Detect, respond to, and contain security threats.

Key Activities:

- SOC Monitoring
- Threat Detection
- Incident Response
- Threat Hunting

Measures: How quickly can we detect and respond?

PURPLE TEAM

Bridge Attack & Defense

Objective:
Improve security effectiveness through collaboration between attackers and defenders.

Key Activities:

- Detection Engineering
- Security Validation
- Attack Path Testing
- Continuous Improvement

Measures: How effectively do our defenses perform against real attacks?

VISUAL COMPARISON

Team	Core Role	Focus	Outcome
Red Team	Simulate attackers	Identify exploitable gaps	Exposure visibility
Blue Team	Defend systems	Detect & respond to threats	Operational resilience
Purple Team	Align offense & defense	Improve security effectivenes	Continuous optimization

Selecting the Right Testing Approach

01 Red Teaming

Best suited for organizations seeking to understand how attackers could breach systems, applications, or infrastructure.

02 Blue Team

Ideal for organizations focused on strengthening monitoring, detection, and incident response capabilities.

03 Purple Team

Recommended for organizations aiming to continuously validate and improve security controls and SOC effectiveness.

Final Perspective

Modern cybersecurity requires more than isolated offensive or defensive testing. Organizations need continuous validation, operational visibility, and collaborative security improvement to remain resilient against evolving threats.