Q Recently I heard the term "purple team." What are the objectives and roles of this team?

A Organizations need proactive measures for ensuring that information and cybersecurity teams are constantly prepared to defend the organization from attacks from existing and emerging threats. Part of those measures include teams to carry out various activities required for defending the organization from such attacks. These teams are organized into red, blue and purple teams. Originally, there were only red and blue teams. Purple teams are the most recent addition to these teams.

Red teams are the attackers. Red teams are a group of security professionals who are well versed in attack methods and knowledgeable about how to break into systems. The members of this team can be internal employees or third-party contractors or consultants. The advantage of using third-party contractors is that the team members are not aware of the security controls. However, due to their lack of inside knowledge, they might overlook or miss certain vulnerabilities. Some organizations use internal red teams that are supported by third-party contractors to provide independent testing. Red team members must be knowledgeable about all forms of cyberattacks and social engineering methods to find ways to break into systems. Team members must sign nondisclosure agreements.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, CDPSE, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

Blue teams are the defenders. Blue teams detect and defend the attacks by red teams. Generally, the team members are employees of the organization; however, small organizations that engage contractors to manage their IT and security operations may engage third-party contractors.

Blue teams have the dual responsibilities of continually hardening security and defending systems from attacks. This is essential because red teams may attack unannounced, just as real attackers do.

Red and blue teams work together to provide a complete review and audit of security systems. They review all attacks and the reasons for any successful attack. The red team provides detailed logs of all attack operations performed and the blue team completely documents all findings and actions taken.

There is clear distinction in roles for red (attackers) and blue (defenders) teams; however, purple teams may mean different things to different security professionals.

According to some, the role of a purple team is more of a coordination performed by normal users (end users and supervisors). The purple team is made aware of the possible threats and tries to identify them when the red team attacks. If the purple team fails to detect an attack, blue teams must detect and defend. In essence, the need for an extra line of defense has resulted in the formation of purple teams. An organization, therefore, typically places purple teams somewhere between the first and second lines of defense and blue teams between the second and third lines of defense.

Other organizations use purple teams to harden defenses and test security, which is the responsibility of a single group of people who perform functions of both red and blue teams. In these cases, purple teams can be IT security consultants, auditors or employees. Team members often take turns performing attacks and defenses, which helps sharpen skills. Purple teams can also perform spot checking of security tools.

However purple teams are implemented in an organization, they support the red and blue teams to strengthen security.