InfoSight
Bringing the Future into Focus
305-828-1003
info@infosightinc.com
www.infosightinc.com

InfoSight's Red, Blue & Purple Team Testing

InfoSight performs Red Team, Blue Team, and/or Purple Team Testing for organizations to assist in vulnerability detection, threat hunting, and network monitoring by accurately simulating common threat scenarios and facilitating the creation of new techniques designed to prevent and detect new types of threats. Each testing is unique to your organization and takes a strategic approach to establish the effectiveness of your systems and network's security posture.

So, what's the difference?

Red Team Testing services utilize a strategic approach towards an organization to test the resilience of the target using custom sophisticated attacks. InfoSight imitates persistent, motivated, and heavily resourced attackers by using advanced tactics, techniques, and procedures to penetrate the organization and achieve realistic goals.

This method of assessment is geared towards clients with a mature and highly evolved security posture. This is the highest capability testing level from an assailant and resistance maturity standpoint, which classifies methodological, technical, and behavioral security control weaknesses. Red Team testing elevates an already mature security-aware organization by exercising all aspects of their prevention, detection, and response capabilities and demonstrates the return on their investment in security.

Blue Team Testing services include a team of incident responders who sit with your security personnel and use your existing tools to identify, assess and respond to the intrusion. During the testing phase, the Red Team will notify the Blue Team before each phase begins allowing your incident responders to use the actual tools in your environment to track and attempt to disrupt attacker activity. After each phase concludes, we review both teams' actions, identifying what responders did well, what could be improved, and whether any gaps exist that should be highlighted.

Purple Team Testing services combine red and blue teams and allow both teams to work closely together to maximize cyber capabilities through continuous feedback and knowledge transfer. Some organizations perform purple teaming as one-off focused engagements, whereby security goals, timelines, and key deliverables are clearly defined, and there is a formal process for evaluating lessons learned over the course of an operation.

This includes recognizing offensive and defensive shortcomings and outlining future training and technological requirements. An alternative approach gaining traction in the security market is to view purple teaming as a conceptual framework that runs throughout an organization, establishing permanent communication channels and fostering a collaborative and transparent culture that promotes continuous cybersecurity improvement.

InfoSight
Bringing the Future into Focus
305-828-1003
info@infosightinc.com
www.infosightinc.com

InfoSight's Red, Blue & Purple Team Testing

The goals and approaches between Red Team, Blue Team and Purple Team testing vary. Check out our chart below for an easy to read breakdown!

	Red Team	Blue Team	Purple Team
Goals	• Confirm the overall strength of an organizations defense • Give valuable insight into the security posture of assets • This allows the hardening of controls and eliminates any weaknesses before hackers can cause serious damage by exploiting those weaknesses	• Brings value to an organization by strengthening its defenses against cyber-attacks. • Identify oversights in the network's visibility or defenses and provide suggestions for improvement.	• Ensure and maximize the effectiveness of the Red and Blue teams. • Facilitate this continuous integration between the two groups, which fails to address the core problem of the Red and Blue teams not sharing information.
Approach	• One-Off: A one-off assessment that exhausts the entire attack path of a successful compromise. • Retained Red Teaming: The Red Team can act as on retainer to launch a certain number of unannounced and targeted campaigns over a set period of time • Rebel Team (Blue Team Integration): Working closely with members of the organization's internal blue team, stages in the attack path are simulated to assure that the appropriate detection mechanisms are effective.	• Helps your personnel detect adversary reconnaissance and consider preventive measures that can be taken in response. • Works with your security personnel to triage the incident, conducting host and network-based analysis and identifying the source and destination of the attack, exploitation method, rogue processes, and level of privileged access • Helps your security personnel identify this traffic and search for other potential points of compromise to gain a more comprehensive picture of the attacker's access.	• Combination of both the Red and Blue team ensures constant communication and information flow. • Provides emphasis on remediation of vulnerabilities rather than prevention and detection growth • Pairing a tester and responder together for improved results. • Scenario based assessment services • Evaluates the effectiveness and proper implementation of applications