InfoSight®
www.infosightinc.com

INFOSIGHT'S RED, BLUE & PURPLE TEAM TESTING

305-828-1003 info@infosightinc.com

Our Red Team, Blue Team, and Purple Team Testing assist organizations in vulnerability detection and threat hunting by accurately simulating common threat scenarios. The goal is to collaborate with your team to identify and defend your organization from different types of threats. The testing plan is unique to your organization's operational environment and existing attack surface. We take a strategic approach to the planning but employ tactical expertise to execute the testing.

So, what’s the difference?

Red Team Testing

Red Team Testing services imitate motivated and well resourced attackers by using advanced tactics, techniques, and tools to compromise systems with zero knowledge. This method of assessment is geared towards mature environments with a highly evolved security culture. This is a realistic adversary attack simulation of a bad actor and will identify 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

Blue Team Testing focuses on assessing and improving your organization's defense mechanisms and incident response capabilities. It involves simulating various cyber threats and attacks to evaluate how well an organization's security team, processes, detects, responds to, and mitigates these threats effectively. It plays a vital role in enhancing an organization's overall cybersecurity resilience by identifying weaknesses and facilitating improvements in security measures.

Purple Team Testing

Purple Team Testing is collaborative cybersecurity testing approach with your team that combines elements of both red teaming and blue teaming. It focuses on improving an organization's overall security posture by enhancing communication and cooperation between the offensive (red) and defensive (blue) security teams. Purple team testing is designed to ensure that both teams work together effectively to identify vulnerabilities, test security controls, and improve incident detection and response capabilities. Purple team testing bridges the gap between offensive and defensive cybersecurity activities. It promotes a proactive and cooperative approach to cybersecurity by ensuring that the red and blue teams work together to strengthen the organization's security defenses, identify vulnerabilities, and enhance incident response capabilities.

Bringing the Future into Focus

www.infosightinc.com

INFOSIGHT'S RED, BLUE & PURPLE TEAM TESTING

The goals and approaches between Red Team, Blue Team and Purple Team testing vary

	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 is 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.	➡ A 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