InfoSight®
www.infosightinc.com



Offensive & Defensive Security Testing

Red, Blue & Purple Team Testing

Simulate real attacks, sharpen real defenses, and prove real ROI on your security investment.

www.infosightinc.com | info@infosightinc.com | 305-828-1003

So, What's the Difference?

Same mission — different lens on your defenses.

Red Team

Attack, unannounced.

A zero-knowledge simulation of a motivated, well-resourced adversary using real-world tactics and tools. Built for mature, security-aware organizations, it stress-tests prevention, detection, and response — and proves the ROI on your security investment.

Best for validation
Mature, security-aware organizations proving real-world resilience.

Blue Team

Defend, and improve.

Assesses and strengthens your defenses and incident response by simulating attacks against your security team's processes. Identifies weaknesses and drives measurable improvement in detection and response.

Best for readiness
Teams strengthening detection, response, and analyst skill.

Purple Team

Collaborate, in real time.

Pairs your red and blue teams in a live, coordinated exercise. Closes the information gap between offense and defense — testing controls, improving detection, and strengthening response together.

Best for collaboration
Organizations aligning offense and defense in real time.

Every engagement is scoped to your environment, your attack surface, and your existing security maturity.

Goals and approach differ by engagement type — here's how each one plays out.

Red Team	Blue Team	Purple Team
Goals		
Confirm the real-world strength of your defenses and expose control weaknesses before attackers do — validating ROI on security investment.	Strengthen defenses against live attack scenarios; surface visibility gaps and concrete improvement opportunities across people, process, and tooling.	Maximize the effectiveness of both Red and Blue by closing the information gap between offense and defense — so lessons translate into hardened controls immediately.
Approach		
One-off: a single engagement that exhausts a full attack path end to end. **Retained:** ongoing, unannounced campaigns on a set cadence to keep defenses honest over time.	Detects adversary reconnaissance and recommends preventive measures. Triages incidents through host and network analysis — source, destination, exploitation method, and privilege level — to build a full picture of attacker access.	Pairs a tester and a responder together in real time. Scenario-based exercises validate detection and response as controls are actively tested — not after the fact.

Why Run It With InfoSight

- ✓ **Real operators, not scripts** — senior engineers plan and execute every engagement.
- ✓ **Scoped to your environment —** testing plans built around your actual attack surface.
- ✓ **Tracked in Mitigator —** findings and retests live in one platform for ongoing visibility.

Certified Expertise

OSCP | OSWP | CISSP | CCSP | CISA | CISM | CEH | CHFI | CPENT | LPT | Security+ | PenTest+ | CySA+ | Cloud+ | eJPT | eCPPT | AWS Security | AWS Networking | CCNA | CCFP | DRI | CARTP

Ready to see how your defenses hold up?

Schedule a Red, Blue, or Purple Team engagement with InfoSight.