LevelBlue

Red Team Assessments

Test your resilience with a risk-controlled attack.

Why Red Team testing?

LevelBlue Red Team Assessments strengthen a mature, security-conscious organization by testing all facets of their prevention, detection, and response capabilities — while demonstrating the return on their investment in security.

The LevelBlue Red Team methodology offers customized, intelligence-driven cybersecurity assessments that are carefully managed. These tests simulate the behaviors of threat actors who pose a real threat to critically important assets (goals and trophies).

What we deliver

- Realistically simulate attack scenarios identified by our threat intel team, including advanced phishing and whaling, insider threat simulation, and customized scenarios designed to compromise the client's critical systems, data, or other objectives.
- Assist clients in identifying and evaluating their existing compromise detection controls, incident response and/or management, and breach-reporting processes.
- Identify vulnerable systems, missing security controls, and potential detection blind spots.

Given the variability of tactics, techniques, and procedures used by adversaries, LevelBlue Red Team Assessments can focus on customized scenarios supported by threat intelligence.

While these scenarios are tailored for each client Assessment, they can often be grouped into the following categories:

Advanced External Attacker

This test simulates the potential impact of an unauthenticated user conducting persistent attacks, including advanced network or application-level assaults, password spraying, phishing, vishing, wireless, physical, and other identified potential attack avenues.

Compromise Simulation and/or Insider Threat

This test mimics the potential effects of a malicious insider with authenticated access, a skilled end-user, or a host compromised by malware or stolen credentials. By pretending to be a legitimate user with low-level domain privileges, LevelBlue can simulate a targeted attack, attempting to bypass security controls and access restricted data and internal systems.

The LevelBlue Red Team approach

LevelBlue's Red Team testing assesses an organization's resilience against sophisticated, targeted attacks by simulating highly motivated and well-resourced adversaries using advanced tactics, techniques, and procedures. This outcome-focused approach aims to identify weaknesses in technical, procedural, and behavioral security controls, enabling organizations to proactively strengthen their security posture and better protect their assets against real-world threats.

Elite testing team

LevelBlue's team sets itself apart with a unique dual perspective—we are the same experts who investigate the most advanced cyberattacks and develop defenses to prevent them. Our global professionals hold industry-leading certifications, including CREST, CISSP, GSEC, GCIH, GPEN, GCTI, OSCP, and CFE, offering extensive expertise in both proactive risk consulting and reactive incident response. With 24×7 coverage and established relationships with over 40 cyber insurance panels, we don't just respond to cyber threats—we help organizations build lasting resilience that adapts to the evolving threat landscape, turning real-world attack intelligence into actionable defense strategies that protect what matters most.