RED TEAM EXERCISE

What are Red Team Engagements?

Red team engagements simulate real adversaries attempting to achieve specific objectives in your environment beyond a standard penetration test (e.g. exfiltrating data, maintaining persistent access). Unlike penetration tests that find vulnerabilities within a defined scope, red teams use every available vector (technical, physical, social engineering) to test whether your organization can detect and stop a determined attacker.

These are weeks, or months-long, engagements conducted with zero knowledge and maximum stealth, mirroring advanced persistent threat (APT) tactics. Your security team doesn't know it's happening, which reveals whether your defenses actually work when it matters.

What Makes Red Teaming Different:

Goal-Oriented, Not Checklist-Driven

We're not finding every vulnerability, we're achieving specific objectives you define, using whatever methods real attackers would use. This tests your defenses in realistic scenarios, not theoretical ones.

Multi-Vector Attack Simulation

We combine technical exploitation, social engineering, and physical access attempts. Real adversaries don't limit themselves to one attack surface, so neither do we.

Detection and Response Validation

The primary value isn't discovering vulnerabilities, it's testing whether your security team, tools, and processes can detect and respond to sophisticated threats before damage occurs.

Stealth and Evasion

Informed by active incident response work, we use the same evasion techniques we see adversaries employ in real breaches. This tests your defenses against current tradecraft, not outdated attack methods.

Who Benefits from Red Team Engagements?

Organizations with mature security programs that have conducted multiple penetration tests and want to validate their detection and response capabilities. Red teaming answers critical questions: Can your SOC identify a breach in progress? Do your IR procedures work under real conditions? Are your security investments delivering the protection leadership expects?

Why Use SEVN-X for Red Team Engagements?

Our red team operators respond to real breaches weekly. We don't just study attack techniques. We observe them during active incident response, then replicate them to test your defenses. When you need to know if your organization can stop a determined adversary, you need testers who think and operate like one.

info@sevnx.com

484.989.0911

ACHIEVE BETTER CYBERSECURITY