SEVNX

SERVICE BRIEF · ADVERSARY EMULATION

RED TEAM EXERCISE

A determined, goal-driven attack that tests whether you can detect and stop a real adversary.

A red team engagement goes well beyond a penetration test. We act as a real adversary pursuing the objectives you define, using every vector available, technical, physical, and social, with zero knowledge and maximum stealth. **Your** security team **should not** know it is happening **to determain whether your defenses actually work when it matters**

WHAT MAKES IT DIFFERENT

Goal-Oriented, Not Checklist-Driven

We pursue specific objectives you define, the way real attackers would, testing realistic scenarios instead of theoretical ones.

Multi-Vector Attack

We combine technical exploitation, social engineering, and physical access, because real attack adversaries never limit themselves to one surface.

Detection & Response Validation

The real value is true threat replication. No time constraints, no lowering the shields, no whitelists.

Stealth & Evasion

We use the same evasion tradecraft we see adversaries employ in real breaches, against your current defenses.

WHY SEVN-X

Our red team operators evaluate real breaches every week. We do not just study attacker techniques, we watch them during live incident response and replicate them against your defenses. **To know if you can stop a determined adversary, you want testers who operate like one.**

- Zero-knowledge, full stealth
- Built for mature programs
- APT-style tradecraft