TEVORA

One Spectrum Pointe Drive, Suite 200
Lake Forest, California 92630
t: 949.250.3290 | **e:** info@tevora.com

RED TEAM ATTACK SIMULATION

Guarding your organization's assets can be a vast undertaking. Tevora's elite threat team combines years of industry experience with exceptional outside-the-box thinking skills and industry certifications to provide you with the answers you need. By going beyond simple automation tools testing, we can help you understand whether your current controls are effective in protecting you from external and internal threats.

STRIKE FIRST

Tevora's Red Team attack exercise will simulate a malicious attack, allowing you to fully understand and test the effectiveness of your defenses against a sophisticated stealth adversary. Every Tevora Red Team attack simulation is customized to your organization's environment, ensuring an effective, thorough and disruption-free assessment. We offer two main testing scenarios:

BLACK BOX TESTING

- The Tevora Red Team will be provided with little to no information of the testing environment
- Attack vectors will be discovered through comprehensive reconnaissance
- Knowledge level of unaffiliated attacker will be simulated

WHITE BOX TESTING – AKA PURPLE TEAMING

- Tevora's Red Team will collaborate with your team (Blue Team) to design a custom test for your environment
- Testing will focus on areas identified to be potentially vulnerable
- All black box discovery efforts will also be conducted
- Enables discovery of hard to identify threats

1 RECON

- **Data exfiltration and open-source intelligent gathering**
- **Network enumeration and service footprinting**
- **Stealthy exploitation of vulnerable systems**
- **Mapping and exploitation of externally facing assets**
- **Email and phone phishing**

2 ASSESS

- **Emulation of known attack patterns and vectors**
- **Mapping and exploitation of externally-facing assets**
- **Thorough passive information gathering and public record analysis**
- **Known vulnerability identification**
- **Exploit development and execution**
- **Pivoting and escalation of access**
- **Social engineering campaigns against target employees**

3 REPORT

- **Collaborative debrief session**
- **Executive Summary**
- **Detailed findings report with recommended remediation**
- **Retesting with validation**
- **Executive presentation**