TEVORA

tevora.com

Threat Management

Red Team Attack Simulation

Cybercriminals constantly evolve their attack tactics and digital attributes in order to bypass the latest security controls and exploit vulnerabilities in systems, software, and endpoints. In this challenging threat environment, you need a partner that can help you manage your risk.

Tevora IS that partner. Our certified and experienced engineers proactively **test** your IT environment to uncover security risks, **remediate** existing threats and vulnerabilities, **assess** compliance with industry security requirements and **train** users on security awareness. If you suspect a compromise, Tevora's elite team can **isolate** the threat, **clean** the system, and **build** your defenses to help protect against future attacks. ▲

"Red teaming" is a term borrowed from military war games and adapted to the business environment to test force-readiness for a variety of situations. In Tevora's Red Team Attack Simulations, we conduct a covert attack on your organization to test the effectiveness of security controls against a sophisticated stealth adversary. The exercise provides a real-world view of your security posture from the attacker's perspective, which allows you to "strike first" to find and fix your security weaknesses before an attacker exploits them.

Tevora's Red Team Attack Simulation Process

1. Reconnaissance

- Perform discovery efforts including:
  - — Data exfiltration and open source intelligent gathering
  - — Network enumeration and service footprinting
- Conduct stealthy exploitation of vulnerable systems
- Map and exploit externally facing assets
- Run phishing (email) and vishing (phone) campaigns

2. Assessment

- Emulate known attack patterns and vectors
- Map and exploit externally facing assets
- Conduct thorough passive information gathering and public record analysis
- Identify known vulnerabilities
- Develop and execute exploits
- Pivot and escalate access
- Conduct social engineering campaigns against target employees

3. Report

- Conduct a collaborative debrief session
- Provide a detailed findings report with recommended remediation
- Retest with validation
- Present findings to executive team
- Create an executive summary of findings for management

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Lake Forest, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and –year after year –apply our cumulative learnings to continually strengthen the company's digital defenses.

Go forward.
We've got your back.

Two testing scenarios are offered in Tevora's Red Team Attack Simulations:

Black box testing

The Tevora Red Team is provided with little or no information of the internal structure or design of the environment being tested. Attack vectors are discovered through comprehensive reconnaissance that includes open source intelligence gathering. The knowledge-level of an unaffiliated attacker is simulated.

White box testing (a.k.a. purple testing)

Tevora's Red Team collaborates with your Blue Team to design a custom test for your environment. Testing focuses on areas that are identified as potentially vulnerable, and enables the discovery of hard-to-identify threats. Attack vectors are discovered through the same efforts as in our black box testing.

Every Tevora Red Team Attack Simulation is customized to your organization's environment to ensure an effective, thorough and disruption-free assessment.