TEVORA

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

APPLICATION PENETRATION TESTING

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.

PROTECT YOUR BUSINESS FROM COMPROMISE – Attackers can leverage security flaws in mobile and web applications, and Application Programming Interfaces (APIs) to gain access to sensitive resources, leaked data and even acquire remote access to internal servers. Tevora's elite threat team employs a rigorous testing process to analyze your applications and create a customized plan to help improve security posture.

WEB APPLICATION PENETRATION TESTING – Web applications are generally open to the entire internet, with an unknown sum of attackers and bots scanning for weaknesses. Tevora's elite threat team can perform manual tests to validate that your application is secure and that it aligns with your business needs. The result is a report that helps guide your development team to remediate any discovered issues.

MOBILE APPLICATION PENETRATION TESTING – Tevora will simulate a real-world attack against your mobile app in a controlled and safe environment. Using thorough testing techniques, Tevora's elite threat team will determine whether security controls have been properly executed and if they will be effective against an attack.

API PENETRATION TESTING – APIs provide powerful windows into your data, but are often targets for attackers. Tevora offers whitebox API testing to ensure the security model of APIs are enforced across all platforms. By performing threat modeling, Tevora 's elite threat team is able to identify any potential attacks and showcase the impact they can have on your business.

1 RECON

- Whitebox testing
- Enumeration of URLs and endpoints
- Open-source intelligence gathering
- Client-side application analysis

2 ASSESS

- Identification of known vulnerabilities
- Testing input validation
- Use of latest OWASP testing guidelines
- Application logic testing
- Authentication, authorization and session management

3 REPORT

- Executive summary for management
- Detailed findings report with recommended remediation
- Retesting with validation
- Executive presentation
- 3rd party reporting