TEVORA™

tevora.com

Threat Management

Application Penetration Testing

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.▲

Building secure applications can be a challenge even for the most seasoned developer. While secure coding practices, regular security testing and code reviews, and other best practices can minimize an application's risks, many flaws go undetected. The potential for exploitation of these vulnerabilities is high, as motivated attackers actively seek out and leverage an application's internal structural weaknesses in order to gain unauthorized access to an organization's sensitive resources, leaked data, and internal servers.

HITRUST Authorized CSF Assessor

Tevora's Application Penetration Testing Process

1. Reconnaissance

- Examine the internal application design, structure, coding and security controls using white-box testing
- Gather open-source intelligence
- Analyze client-side applications

2. Assessment

- Follow current OWASP testing guidelines
- Identify known vulnerabilities
- Test input validation
- Perform application logic testing
- Assess authentication, authorization and session management
- Evaluate mobile device management containerization and application protection on rooted or jailbroken devices (mobile application-specific)
- Apply threat modeling to the identified vulnerabilities to determine potential business impact

3. Reporting

- Prepare a detailed findings report based on the testing that:
  - includes steps and conditions of the testing so that it is repeatable
  - recommends approach to remediation
  - defines a customized plan to improve application security posture
- Include any relevant third-party security preparedness (SOC 2 reports, ISO certifications, etc.)
- Communicate findings to leadership and stakeholders that provides a clear overall assessment
- Retest after remediation with validation

TEVORA™

tevora.com

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

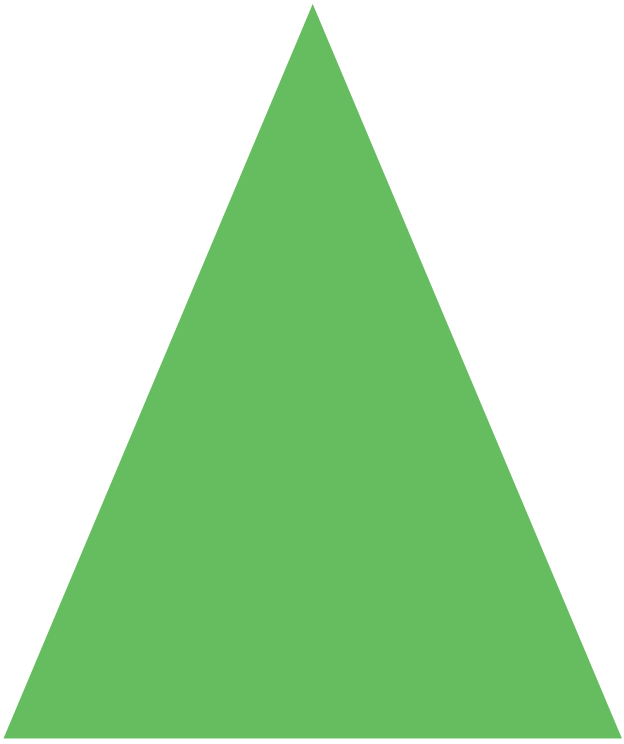
Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Lake Forest, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure 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.

Tevora partners with you to surface and remediate existing application security risks proactively – before an attacker exploits them. Our elite threat team performs rigorous application penetration testing that simulates real-world threats and attacks in a controlled, safe environment on your **web, mobile** (Apple iOS and Google Android platforms) and **desktop applications**; and backend **application programming interfaces** (APIs). Penetration testing helps us determine whether security controls are executed properly within the software's internal structure, and if they will be effective against an attack.

Additional testing methods include white-box testing, which allows our experts to assess the integrity of the application's "inner" workings (e.g., design, structure and coding), and whether an API's security model is enforced across all platforms. If exposures are identified during any testing, the Tevora team uses threat modeling to determine their potential impact on your business. A detailed findings report includes our remediation recommendations and defines a customized plan to help you improve your application security posture.



HITRUST Authorized CSF Assessor