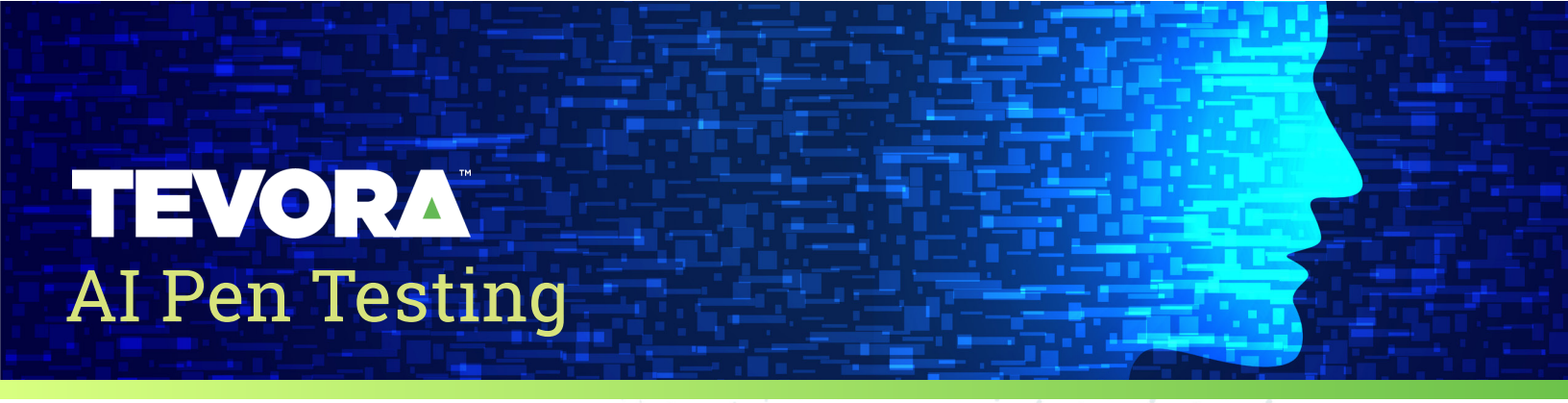
TEVORA™

AI Pen Testing



As organizations rapidly adopt AI-driven applications, security teams face new challenges that extend beyond traditional application testing. Large Language Models (LLMs) introduce unique attack surfaces, including prompt manipulation, data leakage, model misuse, and unpredictable system behavior. Aligning PTES, OWASP Testing Practices, and the OWASP LLM Top 10 to Address Modern Application and AI Risk

CREST | PEN TEST

Our CREST-certified penetration testing team combines offensive security expertise with emerging AI threat knowledge to uncover vulnerabilities across models, APIs, integrations, and infrastructure.

The Tevora Approach

1 Planning & Preparation

A collaborative process designed to align testing with your AI use cases, risk profile, and business objectives

Key Outputs:

- Define scope across LLM applications, APIs, plugins, and third-party integrations
- Establish testing objectives based on real-world threat scenarios
- Align on rules of engagement, constraints, and success criteria

2 Reconnaissance

Understanding how your AI system behaves, responds, and interacts with users and connected services.

Key Outputs:

- Map AI system architecture and exposed interfaces
- Identify data sources, retrieval mechanisms, and external integrations
- Assess potential exposure points across APIs and user inputs

3 Known Vulnerability Identification

Evaluating both traditional application weaknesses and emerging AI-specific risks.

Key Outputs:

- Test for common web and API vulnerabilities (OWASP-aligned)
- Identify misconfigurations in AI services and infrastructure
- Evaluate known LLM risks such as prompt injection and data leakage

4 Adversarial Testing & Behavioral Analysis

Simulating real-world attacker techniques to understand how the system can be manipulated or influenced.

Key Outputs:

- Test model behavior under adversarial inputs and manipulated context
- Evaluate data exfiltration risks through indirect prompt paths
- Analyze cascading impacts across integrated systems and workflows

5 Reporting

Turning technical findings into clear, actionable intelligence for security, engineering, and executive stakeholders.

Key Outputs:

- Technical breakdown of vulnerabilities and exploit paths
- AI-specific risk categorization and impact assessment
- Strategic recommendations for improving long-term AI security posture

Go forward.
We've got your back.

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's organizations, people, and 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.

ACHIEVED ACCREDITATIONS

ISO 27001 Lead Auditor · ISO 27017 Certified · ACCREDITED CERT #5062.01 · CREST PEN TEST

ACHIEVED ASSESSOR

PCI Security Standards Council — PCI DSS QSA, PCI PA-DSS QSA, 3DS ASSESSOR · AICPA SOC · ISO Audit · HITRUST Authorized CSF Assessor · FedRAMP · TRUSTED PARTNER NETWORK · GovRAMP

AI SECURITY STRATEGY

Artificial Intelligence has prompted a new landscape of compliance frameworks, threat vectors, and security tools. We make it our job to understand and pioneer the security programs that account for—and take advantage of—all that AI brings to the table.

COMPLIANCE

The assessment is only the first step of your compliance journey. We'll help you understand your path to achieving and maintaining continuous compliance against the security and privacy frameworks you need to do business.

THREAT MANAGEMENT & RESPONSE

Whether proactive or in case of emergency, Tevora has your back in the face of threat actors. We offer comprehensive and targeted penetration testing, social engineering, and other tactics to find gaps before others can exploit them.

SECURITY INFRASTRUCTURE

Tevora takes a vendor-agnostic stance to help companies find the best fit software solutions for their security needs. And with knowledge of hundreds of solutions vendors across dozens of categories, we'll help you find your fit.

RISK & STRATEGIC SERVICES

Address risks before they become an issue. Proactive and comprehensive exercise to find and address weaknesses in your security program through Enterprise Risk Management, Third Party Risk Management, Business Continuity and Disaster Recovery exercises, and more.

RESOURCE AUGMENTATION

The complex and specialized work required by cybersecurity and compliance programs sometimes require a focused, expert resource. Tevora can supplement your internal team with flexible Governance, Risk & Compliance (GRC) support, expert DevSecOps support, or even executive-level CISO assistance.