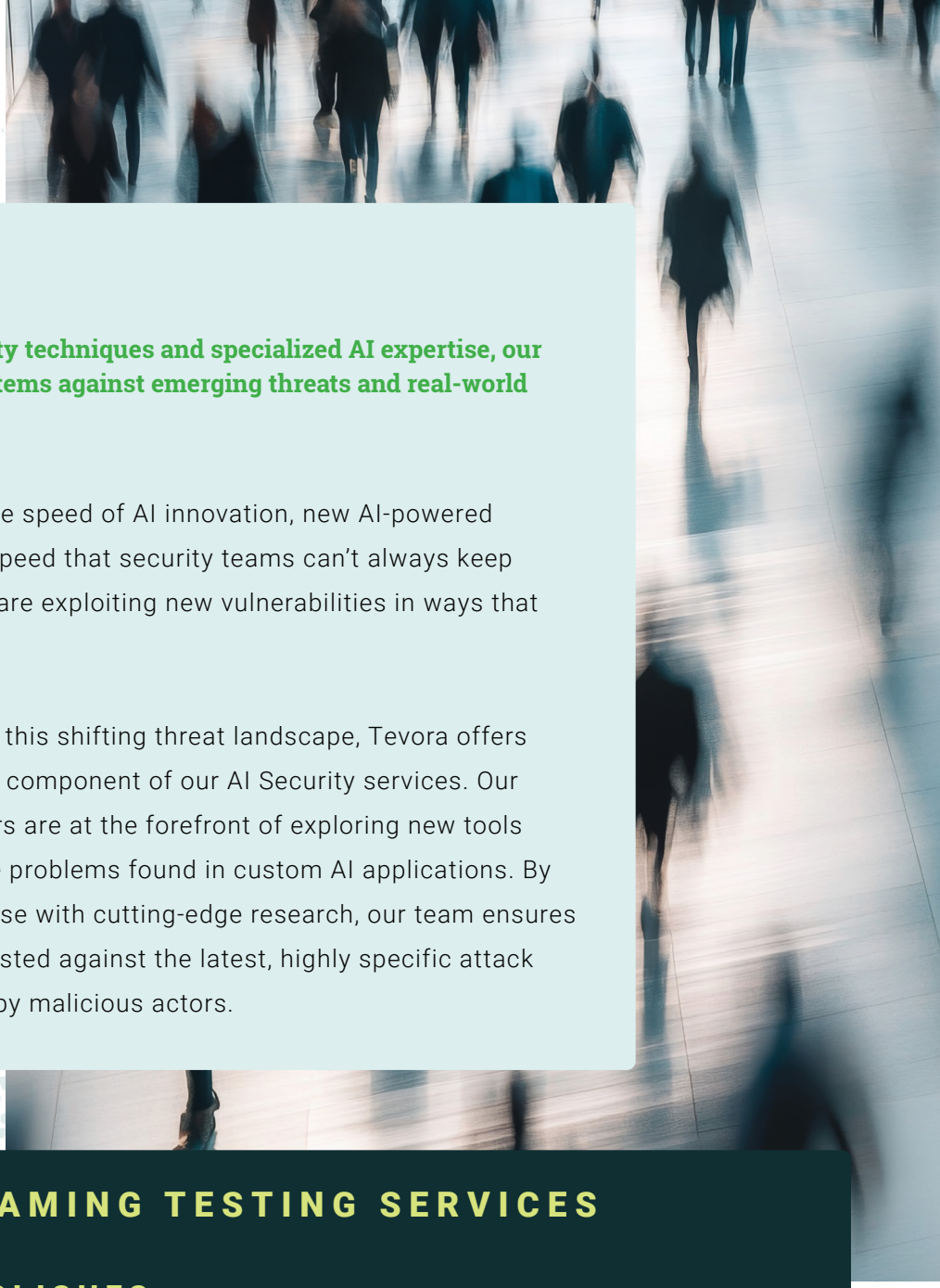
TEVORA™



AI Red Teaming

Leveraging advanced offensive security techniques and specialized AI expertise, our team assesses the resilience of AI systems against emerging threats and real-world attack scenarios.

As companies race to keep up with the speed of AI innovation, new AI-powered applications are being released at a speed that security teams can't always keep up with. Threat actors know this and are exploiting new vulnerabilities in ways that companies did not anticipate.

To help organizations safely navigate this shifting threat landscape, Tevora offers specialized AI Red Teaming as a core component of our AI Security services. Our senior, experienced penetration testers are at the forefront of exploring new tools and techniques to address the unique problems found in custom AI applications. By combining deep cybersecurity expertise with cutting-edge research, our team ensures your AI deployments are rigorously tested against the latest, highly specific attack vectors before they can be exploited by malicious actors.

AI RED TEAMING TESTING SERVICES

WHAT IT ACCOMPLISHES:

Validating that AI applications can withstand real-world attacks and operate securely in production environments

BEST FOR:

Organizations seeking to identify and mitigate security risks within AI applications and models

TESTING METHODOLOGY:

- Map the AI ecosystem, including models, data flows, integrations, and dependencies, to understand the attack surface
- Conduct targeted security testing against AI models and infrastructure to uncover exploitable vulnerabilities and control weaknesses
- Provide actionable recommendations to reduce risk, enhance resilience, and support secure AI adoption at scale

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 · A2LA 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 · TPN Trusted Partner Network · FedRAMP · 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.

833-292-1609 TEVORA sales@tevora.com