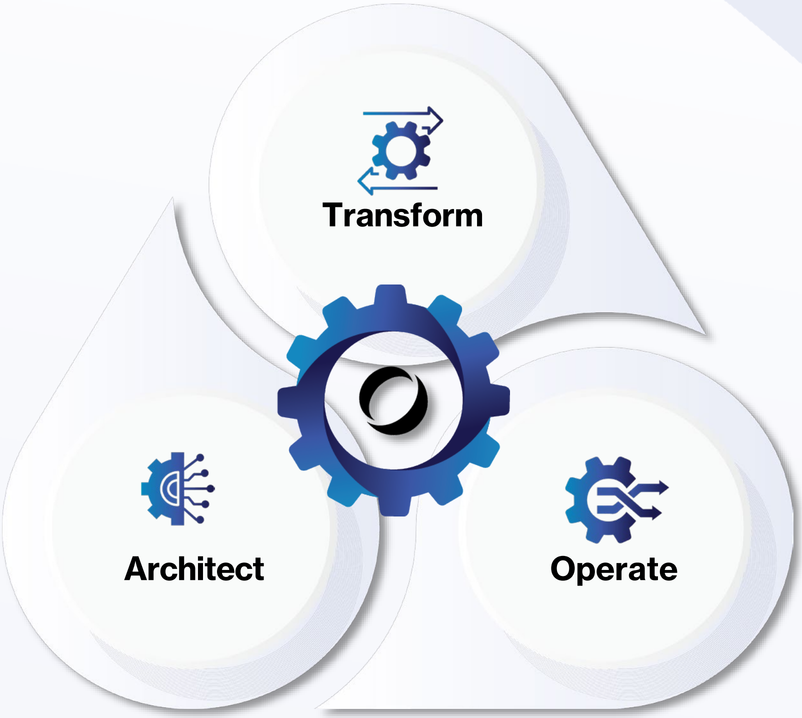
ivision

Security Assessment for AI Enabled Applications

Our Approach

Our Security Assessment for AI-based Applications offering safeguards your AI deployments, concentrating on vulnerabilities specific to Generative AI, such as Prompt Injection and other risks from the OWASP LLM Top 10. We pinpoint potential risks and provide mitigations for your AI-based applications



Common Challenges

- Push from business to launch AI applications quickly
- Risk of AI-enabled data breach or data leakage
- FUD (fear/uncertainty/doubt) around AI and inability to provide answers internally
- Lack of internal expertise around securing AI applications
- 38% of clients say lack of AI expertise/knowledge is their main challenge
- 75% of clients have deployed an AI-enabled application (new or existing)
- 43% of clients’ primary concern with AI is data privacy/security

Benefits

✓ Confidently roll out AI solutions using security best practices

✓ Generate support internally with responsible AI practices

✓ Report on evidence of good security practices for external partners/customers

✓ Reduce risk of AI data leakage/breach

What’s Included

- Application-centric threat modeling
- Zero knowledge to full knowledge application security assessment
- Business impact focused attacks against AI/LLM applications
- Specific remediation advice and support
- Customized training to build a culture of security

Service Options

- Full knowledge or zero knowledge assessment
- Training for team/developers on safe AI implementation
- Ability to focus on customer “flags” (specific engagement goals)

Why ivision?

People

We promote productivity and collaboration through proactive management, clear expectations, and technical expertise.

Process

Our structured and repeatable approach is based on strategic methodology that allows you to capitalize on opportunity.

Technology

Our proven partner ecosystem empowers us to deliver the most innovative solutions for your technology needs.

Contact Us

Any questions on how to get started? Speak with one of our experts.

☎

✉