InterSec
Ignite . Inspire . Innovate

Secure AI Solutions

Harness the power of AI securely, from integration to defense

AI is essential for growth and efficiency—but it also expands your attack surface. InterSec enables you to harness AI safely—accelerate adoption, harden models and data, and counter AI-powered threats with AI.

AI is rapidly transforming the business landscape, offering unprecedented opportunities for innovation and efficiency. Companies are rushing to integrate generative AI, machine learning models, and autonomous systems into their core operations. However, this revolution also introduces a complex and dangerous new attack surface.

Adversaries are keeping pace, leveraging AI to create highly sophisticated attacks, from convincing deepfake-powered social engineering to adaptive malware that evades traditional defenses. They are also targeting AI models directly with data poisoning, evasion, and model-stealing attacks.

This creates a critical dual challenge: how to securely adopt AI technologies without stifling innovation, and how to defend against the next generation of AI-powered threats. Most organizations lack a clear roadmap to navigate this complex, high-stakes environment.

InterSec Inc.'s Secure AI Services solve this problem. We provide an end-to-end expert-led engagement to help you develop the frameworks, test your models, and build the defenses necessary to

Key Benefits

- **Innovate with Confidence:** Deploy powerful AI solutions knowing your data, models, and infrastructure are protected from emerging threats.
- **Stay Ahead of Adversaries**: Proactively defend against next-generation, AI-driven attacks with threat intelligence that understands how attackers think.
- **Ensure Governance & Compliance**: Build and operate your AI systems in alignment with global standards and regulations, such as the NIST AI RMF.
- **Boost SOC Efficiency**: Use AI as a force multiplier for your security team, automating detection and response, not just creating more alerts.

Outcome

InterSec delivers a secure, compliant, and resilient AI program, enabling clients to innovate confidently while protecting their critical initiatives from advanced threats.

InterSec
Ignite . Inspire . Innovate

Services	Description
AI Governance and Compliance Management	We help you navigate AI regulations like the EU AI Act with expert governance frameworks, policy development, and compliance audits.
AI Risk Management	We quantify and mitigate AI risks by identifying technical, ethical, and legal vulnerabilities and providing clear mitigation strategies.
Secure AI Development and Deployment	Our service builds resilient AI models with secure coding and runtime protections to prevent model tampering and adversarial attacks.
Privacy-Preserving AI Solutions	We safeguard sensitive data using techniques like differential privacy and federated learning to ensure compliance and maintain user trust.
AI Security Training	Equip your technical and business teams with hands-on training to secure AI systems against emerging threats.
AI Security Assessments	Our experts identify critical AI vulnerabilities, like prompt injection and data poisoning, using OWASP frameworks to deliver actionable protection insights.
Threat Detection and Response for AI	We monitor and respond to AI-specific threats in real-time, protecting your applications against sophisticated attacks to ensure they remain secure and operational.
Secure Integration of AI with Existing Systems	We securely integrate AI solutions into your existing IT infrastructure using secure APIs and system hardening to ensure compatibility and security.
Ethical AI Auditing and Bias Mitigation	Our audits for fairness, transparency, and bias ensure ethical compliance and build stakeholder trust by enhancing AI reliability.
Continuous Monitoring and Improvement of AI Security	We provide continuous, real-time analytics to address emerging threats, ensuring your AI applications remain protected and adaptable.

Key Features

Our engagement provides a comprehensive, tailored roadmap to secure your AI ecosystem.

Comprehensive AI Security Posture Assessment (ASPA): A deep dive into your existing or planned AI architecture, identifying risks in your data pipelines, models, and deployment processes.

AI Model Vulnerability & Robustness Testing: We test your models against data poisoning, evasion, privacy inference, and extraction attacks to find weaknesses before adversaries do.

Secure AI Integration & Architecture Design: Expert guidance on building a secure foundation for your AI systems, including data governance, access control, and secure MLOps pipelines.

Adversarial AI (Red Team) Emulation: Our experts simulate AI-powered attacks and defenses to test your SOC's readiness against next-generation threats.

AI-Powered Threat Detection Strategy: We help you leverage AI to enhance your own security operations, tuning your systems to find the signals in the noise.

AI Governance & Compliance Framework: We help you develop and implement a practical governance framework that aligns with your business goals and regulatory requirements (NIST, ISO, etc.).

Why Choose InterSec?

Mission-Focused: We have deep experience supporting the critical missions of federal agencies, state governments, and commercial clients, understanding their unique risk profiles.

Expert-Led Teams: Our services are delivered by curated teams of cyber defence engineers and compliance specialists, not just general consultants.

Full Lifecycle Coverage: We provide a holistic program that secures AI from initial governance and development through to real-time threat detection and response.

Actionable & Standards-Based: Our recommendations are practical, actionable, and built on a foundation of globally recognized standards from OWASP, NIST, and ISO.

About Us

InterSec is an expert cyber defence company serving federal agencies, state governments, and commercial clients. Our curated teams of engineers and compliance specialists integrate swiftly into your operations, strengthening risk-sensitive programs and securing your critical AI initiatives.

Learn more: https://www.intersecinc.com
Email: inquiries@intersecinc.com