



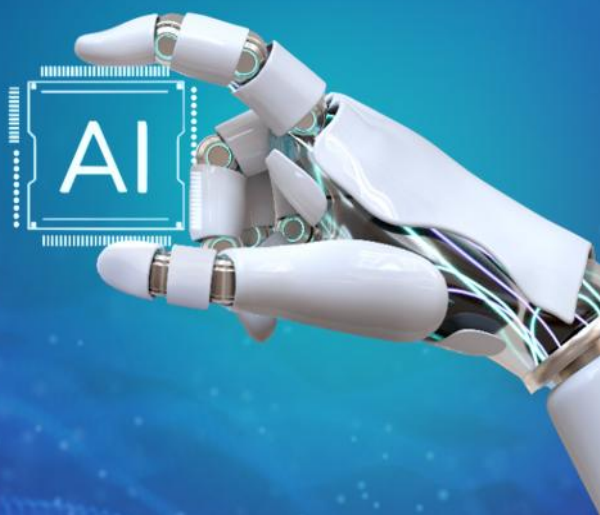
SAFE & SECURE ARTIFICIAL INTELLIGENCE

Artificial Intelligence can revolutionize business operations and unlock competitive advantages. However, it introduces significant security challenges, including data privacy risks, model vulnerabilities, and potential misuse. That's why Sii has developed AI Security Frameworks to help partners identify, assess, and mitigate risks throughout their AI journey.

→ 5 PILLARS OF SECURE AI

When it comes to secure AI projects, five factors stand out:

- 1 **Data Protection:** ensuring sensitive data is properly encrypted, anonymized, and access-controlled throughout the AI lifecycle, including compliance with regulations like GDPR or HIPAA.
- 2 **Bias and Fairness:** building fairness checks, bias detection mechanisms, and transparency features to ensure AI decisions are explainable and don't discriminate against protected groups.
- 3 **Model Security:** protecting AI models from adversarial attacks, data poisoning, and generation of harmful content. This involves robust model validation, version control, and implementing safeguards.
- 4 **Monitoring:** implementing continuous monitoring for anomalous behavior, security incidents, and performance degradation. This includes logging all AI system activities and establishing incident response procedures.
- 5 **Software:** securing the custom serving code and applications that handle AI model inference, including protection against injection attacks, buffer overflows, insecure dependencies, and coding vulnerabilities.



→ WHAT WE OFFER

- AI security coverage aligned with ISO 42001 framework
- Combination of AI model security expertise with IT cybersecurity capabilities
- Complete protection across all layers throughout AI lifecycle
- Compliance with regulations like AI Act

→ WHAT YOU GET?

- Protection of AI investments against emerging threats while maintaining regulatory compliance
- Confidence and agility to scale your AI initiatives without security limitations
- Security, performance, and operational excellence across all your AI systems