

ROLE REFERENCE SHEET

AI Security Architect

AI Security Architect · Securing AI & ML Systems

The architect who designs security controls that protect AI models, data, and pipelines from adversarial and conventional threats across the lifecycle.

WHAT THE ROLE OWNS

- AI security architecture
- AI and LLM threat modeling
- Secure-by-design patterns
- Adversarial testing and red teaming
- Model and data protection
- AI agent security controls
- Detection and monitoring
- Security review of AI systems

FRAMEWORKS

- NIST AI RMF
- MITRE ATLAS
- OWASP Top 10 for LLMs
- ISO/IEC 27001

TYPICAL CERTS

- CISSP · CCSP
- SABSA

8–12+ yrs

Experience

By design

Secure AI architecture

ATLAS

AI threat modeling

**Scan for the free JD template**ai-governance-jobs.com/templates

AGJ, the AI governance job board
Every role hand reviewed since 1999