SCAN FOR THE TEMPLATE

JOB DESCRIPTION TEMPLATE

AI Security Architect

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

Department	Information Security / AI Security / Engineering
Reports to	CISO / Head of Security Architecture
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	8 to 12+ years

POSITION OVERVIEW

The AI Security Architect defines and drives the security architecture for the organization's AI and machine learning systems. This role designs controls that protect models, training data, pipelines, and AI-enabled applications from adversarial and conventional threats.

Working with security engineering, machine learning, platform, and governance teams, the AI Security Architect performs threat modeling, sets security patterns and standards, and reviews AI systems before and after deployment.

As AI moves into production and into agentic workflows, the AI Security Architect ensures AI capabilities are built and operated securely by design.

KEY RESPONSIBILITIES

AI SECURITY ARCHITECTURE

- Define reference architectures and security patterns for AI and LLM systems.
- Set security requirements for model training, deployment, and inference pipelines.
- Design controls for AI agents, tool use, and orchestration.
- Establish secure-by-design standards for AI-enabled applications.

THREAT MODELING AND ASSESSMENT

Perform threat modeling and security assessments of AI systems, addressing risks such as:

- Prompt injection, jailbreaks, and data exfiltration
- Data and model poisoning and supply-chain compromise
- Model theft, inversion, and membership inference
- Insecure output handling and excessive agent permissions

FRAMEWORKS AND STANDARDS

Apply the NIST AI Risk Management Framework, MITRE ATLAS, the OWASP Top 10 for LLM Applications, and ISO/IEC 27001 to shape AI security controls, testing, and standards.

SECURITY REVIEW AND TESTING

- Review AI systems and data flows against security requirements.
- Coordinate red teaming and adversarial testing of models and applications.
- Define logging, monitoring, and detection for AI-specific threats.
- Validate remediation of identified AI security findings.

DATA AND MODEL PROTECTION

- Design controls for training data confidentiality and integrity.
- Set access, secrets, and key management patterns for AI systems.
- Protect model artifacts, weights, and endpoints.
- Address privacy-enhancing and data-minimization techniques.

ADVISORY AND ENABLEMENT

Advise engineering and machine learning teams on secure AI design, contribute to AI security policy and governance, and help build organizational capability in AI security.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Computer Science, Cybersecurity, Information Systems, or a related discipline.

- 8 to 12+ years of experience in security architecture, application or cloud security, or security engineering, including work on AI, machine learning, or data platforms.
- Strong understanding of AI and LLM threat landscapes and secure design.
- Experience with threat modeling, security reviews, and control design.
- Ability to communicate security architecture to technical and business audiences.

PREFERRED CERTIFICATIONS

One or more of: CISSP, CCSP, SABSA, GIAC security certifications, cloud security certifications.

TECHNICAL KNOWLEDGE

AI and LLM security, security architecture, threat modeling, adversarial machine learning, MLOps and pipeline security, cloud and application security, identity and secrets management, red teaming, detection and monitoring, and privacy-enhancing techniques.

ESSENTIAL COMPETENCIES

Architectural thinking, technical influence, clear communication of risk, collaboration with engineering teams, and pragmatic control design.
