NOVARTIS

Associate Director, AI Security Architecture

Job ID
REQ-10090930
Nov 02, 2026
LOC_IL

About the Role

Key Responsibilities

- Lead AI architectural activities and develop secure solution architectures across business and technology domains.
- Define AI security standards and best practices for protecting AI pipelines, datasets, models, and infrastructure.
- Develop logical architecture designs and strategies to secure the organization’s AI domain and infrastructure.
- Establish and evolve AI architecture governance frameworks, including methods, practices, standards, and reusable architecture patterns.
- Assess the AI landscape, identifying and mitigating security risks across model training, deployment, and operations.
- Evaluate AI security technologies and integrate appropriate security controls across AI platforms and Large Language Models.
- Secure AI and agentic systems against model poisoning, adversarial inputs, prompt injection, jailbreaking, and emerging threats.
- Design Model Context Protocol servers, AI agent workflows, secure deployment architectures, and AI gateway integrations.
- Build Python services, developer tools, integrations, and AI security harnesses supporting secure software development.
- Collaborate with data scientists, engineers, and DevOps teams to embed security throughout the AI development lifecycle.

Essential Requirements

- 12+ years of overall professional experience, including substantial experience across security, architecture, software development, and AI security engineering.
- At least 5 years of security experience, 5 years in architecture, 5 years in development, and 2+ years in AI security and engineering.
- Proven AI security architecture expertise covering training data, models, pipelines, deployed AI solutions, security policies, standards, and architecture patterns.
- Strong knowledge of AI threats, risk identification, threat modeling, data privacy, and defenses against adversarial and AI-based attacks.
- Hands-on experience securing Artificial Intelligence and Machine Learning applications across cloud platforms, with strong Amazon Web Services engineering and architecture expertise.
- Production experience with AI coding agents, Model Context Protocol servers, agent workflows, Python development, automated testing, and AI gateway integrations.

Desirable Requirements

- Security engineering or application security background, with experience evaluating and working with specialized AI security technologies.
- Experience building developer-facing command-line tools and working effectively in multi-vendor, global technology environments.

Role Requirements

Division
DIV_TO
Business Unit
Information Technology
Location
LOC_IL
Site
Israel
Company / Legal Entity
IL04 (FCRS = IL004) Novartis Israel
Functional Area
FCT_IT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10090930

Associate Director, AI Security Architecture

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10090930-associate-director-ai-security-architecture*

List of links present in page

1. https://jobapi.novartis.com/req-10090930-associate-director-ai-security-architecture
2. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Associate-Director--AI-Security-Architecture_REQ-10090930
3. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Associate-Director--AI-Security-Architecture_REQ-10090930