NOVARTIS

Associate Director, AI Security Architecture

Job ID
REQ-10090930
Ноя. 02, 2026
Израиль

Сводка

Internal Job Title: Assoc. Dir. DDIT ISC Security Architecture AI
#LI-Hybrid
Location: Israel

Relocation Support: This role is based in Israel. Novartis is unable to offer relocation support: please only apply if accessible.

Help shape how AI can be built, deployed, and scaled securely. In this role, you'll influence the security architecture behind next-Generation AI solutions, defining standards and patterns that protect AI models, data, pipelines, and agentic systems throughout their lifecycle. You'll work at the intersection of AI, cybersecurity, cloud engineering, and architecture, partnering with technical teams to address emerging threats, strengthen secure AI development, and turn evolving security challenges into practical, scalable solutions.

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.

Why Novartis: Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? https://www.novartis.com/about/strategy/people-and-culture

Benefits and Rewards: Learn about all the ways we'll help you thrive personally and professionally.
Read our handbook (PDF 30 MB)

Дивизион
Operations
Business Unit
Information Technology
Место
Израиль
Сайт
Israel
Company / Legal Entity
IL04 (FCRS = IL004) Novartis Israel
Functional Area

Информационные технологии
Job Type
Full time
Employment Type
Regular
Shift Work
No

Job ID
REQ-10090930

Associate Director, AI Security Architecture

Apply to Job

Job ID
REQ-10090930

Associate Director, AI Security Architecture

Apply to Job

Source URL: *https://novartis.ru/careers/career-search/job/details/req-10090930-associate-director-ai-security-architecture*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
3. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Associate-Director--AI-Security-Architecture_REQ-10090930
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Associate-Director--AI-Security-Architecture_REQ-10090930