NOVARTIS

Senior Specialist Security Architecture AI

Job ID
REQ-10090934
Nov 03, 2026
LOC_IN

About the Role

Key Responsibilities

- Shape secure AI architectures, standards and patterns across enterprise AI platforms and solutions.
- Define security strategies protecting AI models, datasets, pipelines and supporting infrastructure.
- Assess AI environments, identify vulnerabilities and mitigate risks throughout the AI lifecycle.
- Design secure agentic AI workflows, Model Context Protocol servers and integrations.
- Embed security into AI development, deployment and Machine Learning Operations processes.
- Develop secure Python services, integrations, web applications and developer-facing tools.
- Build and optimize security scanning capabilities for AI-generated code and software dependencies.
- Evaluate AI security technologies and recommend solutions based on evolving threats and business needs.
- Partner with engineering, data science and platform teams to implement security-by-design practices.
- Communicate AI security risks, architecture decisions and recommendations to technical and senior stakeholders.

Essential Requirements

- Relevant degree or equivalent experience, with substantial professional experience across security, architecture and software development.
- At least 2 years of hands-on experience in Artificial Intelligence security and engineering, including securing models, data and deployments.
- Strong Artificial Intelligence security architecture expertise, including threat modelling, risk identification, security patterns, standards and controls.
- Practical experience securing agentic Artificial Intelligence, including Model Context Protocol integrations, agent workflows and Artificial Intelligence gateways.
- Strong software engineering capability with professional Python development, automated testing and experience using Artificial Intelligence coding agents.
- Strong cloud security and architecture experience, particularly Amazon Web Services, with knowledge of Machine Learning Operations and secure deployment practices.

Desirable Requirements

- Experience with Artificial Intelligence security technologies such as Cranium, Noma, JFrog Xray, HiddenLayer or Darktrace.
- Experience building developer-facing command-line tools and working effectively across global, multi-vendor technology environments.

Commitment to Diversity and Inclusion:

Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

Accessibility and accommodation

Novartis is committed to working with and providing reasonable accommodation to individuals with disabilities. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to perform the essential functions of a position, please send an e-mail to diversityandincl.india@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message

Role Requirements

Division
DIV_TO
Business Unit
Information Technology
Location
LOC_IN
Site
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Functional Area
FCT_IT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10090934

Senior Specialist Security Architecture AI

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10090934-senior-specialist-security-architecture-ai*

List of links present in page

1. https://jobapi.novartis.com/req-10090934-senior-specialist-security-architecture-ai
2. mailto:diversityandincl.india@novartis.com
3. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Senior-Specialist-Security-Architecture-AI_REQ-10090934
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Senior-Specialist-Security-Architecture-AI_REQ-10090934