NOVARTIS

Associate Director, AI Enterprise Security Architecture

Job ID
REQ-10053181

11   24, 2025

Spain

Location: Barcelona, Spain; Tel Aviv, Israel; #LI-Hybrid

Internal job title: Assoc. Dir. DDIT ISC Enterprise Security Architecture – AI

The Enterprise Security Architecture team is looking for an Associate Director, AI Enterprise Security Architecture.

This role you will not just secure algorithms, you will be protecting systems that improve lives worldwide. In Novartis, the ethical dimension of healthcare AI security adds purpose beyond technical excellence.

In particular, you will contribute to the development of AI Security architectural standards, and the direction and design of architecture for a business or technical domain, while contributing to efforts to elaborate and communicate the architecture of the given domain and/or develop architectural solutions for projects and programs. Your voice matters in shaping enterprise AI strategy, not just implementing controls.

About the Role

Key responsibilities:

- Oversee AI architectural activities for a specific business or technology domain, or architectural practice area, and manage the development of solution architectures for projects or programs within a business area.
- Define AI security standards and direction of architecture in the specific business or technical domain, and establish best practices for protecting AI pipelines, datasets, and models.
- Define and develop the logical architectural design and strategies necessary to secure the Organizations' AI domain / infrastructure
- Utilize architecture patterns to suggest the most adequate utilization of technical platforms in support of the holistic AI solution security architecture design.
- Define, create and evolve the Architecture Governance Framework (e.g. architecture methods, practices and standards) for AI.
- Understand and advocate the principles of business and IT strategies, Be prepared to sell the Architecture process, its outcome and ongoing results, and to lead the communication, marketing or educational activities needed to ensure Enterprise Architecture success and use.
- Assess the organization's AI landscape and identifying potential vulnerabilities or weaknesses including identification and evaluation of risks associated with training, deployment, and operation of AI models; keep up-to-date with the latest security threats, trends, and best practices to ensure the AI security infrastructure remains effective, and evaluate and select security tools, technologies, and products to enhance AI security.
- Collaborate with IT teams to integrate security measures into all aspects of the AI platforms and LLMs related processes, working with data scientists, engineers, and DevOps teams to embed security into the AI development lifecycle, and provide guidance and support to other Engineering teams in implementing security measures and resolving security-related issues
- Regularly reporting on the status of AI security measures to senior management and stakeholders.
- Securing AI systems from development through deployment, including securing training data and monitoring deployed models for threats. Knowledge of AI solutions development lifecycle and environments including MLOps and related tooling (e.g. model repositories, data pipelines, deployment architectures).

Essential Requirements:

- University working and thinking level, degree in business/technical area or comparable education/experience
- 15+ years of working experience in Security domain; minimum 5 years in architecture capacity;
- 2+ years of AI Security essential, with expertise in various AI security products (e.g. Cranium, Noma, JFrog X-Ray, HiddenLayer, Darktrace)
- Demonstrated AI security architecture conceptual skills, solutions delivery, and decision making, incorporating sound security principles, from development through deployment, including securing training data and monitoring deployed models for threats
- Prior experience in AI security policy, standards, guidelines, and patterns definition.

- In depth understanding of the AI security domain including strong knowledge of AI threats and mitigating malicious uses of AI and AI risk identification, as well as experience building defenses against AI-based attacks, and enforcing data privacy protocols
- Expertise conducting security design evaluations and threat modeling for AI/ML applications running on cloud platforms like Azure/AWS/GCP.
- Experience in reporting to and communicating with senior level management (with and without IT background), with and without in-depth risk management background on information risk topics, and excellent written and verbal communication and presentation skills; interpersonal and collaborative skills.
- Proven experience to initiate and manage projects that will affect other divisions, departments, and functions, as well as the corporate environment, delivery focused with keen attention to detail and good decision-making ability function with/without supervision to deliver in time and at expected quality.
- Experience working in a multi-vendor, global environment and leading technical teams

Why Novartis?
Our purpose is to reimagine medicine to improve and extend people's lives and our vision is to become the most valued and trusted medicines company in the world. How can we achieve this? With our people. It is our associates that drive us each day to reach our ambitions. Be a part of this mission and join us! Learn more here: https://www.novartis.com/about/strategy/people-and-culture

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to learn more about Novartis and our career opportunities, join the Novartis Network here: https://talentnetwork.novartis.com/network

Accessibility and accommodation:
Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an e-mail to and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

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: Read our handbook to learn about all the ways we'll help you thrive personally and professionally: https://www.novartis.com/careers/benefits-rewards

Operations

Business Unit
Information Technology

Spain

Barcelona Gran Vía

Company /Legal Entity
ES06 (FCRS = ES006) Novartis Farmacéutica, S.A.

Alternative Location 1
Israel, Israel

Functional Area
Technology Transformation

Job Type
Full time

Employment Type
Regular

Shift Work
No

Apply to Job

Job ID
REQ-10053181

Associate Director, AI Enterprise Security Architecture

[Apply to Job](#)

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://www.novartis.com/careers/benefits-rewards
3. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Associate-Director--AI-Enterprise-Security-ArchitectureREQ-10053181
4. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Associate-Director--AI-Enterprise-Security-ArchitectureREQ-10053181