NOVARTIS

AI Enterprise Security Architect

Job ID
REQ-10074087
Mar 13, 2026
LOC_IL

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
- 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
- Experience building defenses against AI-based attacks, and enforcing data privacy protocols
- Expertise conducting security design evaluations and threat modelling 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
- Fluency in English, written and spoken

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.

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

Join our Novartis Network: Not the right Novartis role for you? Sign up to our talent community to stay connected and learn about suitable career opportunities as soon as they come up: https://talentnetwork.novartis.com/network

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

Role Requirements

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)

Division
DIV_TO
Business Unit
Information Technology
Location
LOC_IL
Site
Israel
Company / Legal Entity
IL04 (FCRS = IL004) Novartis Israel
Alternative Location 1
LOC_RO
Alternative Location 2
LOC_ES
Functional Area
FCT_TT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10074087

AI Enterprise Security Architect

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10074087-ai-enterprise-security-architect*

List of links present in page

1. https://jobapi.novartis.com/req-10074087-ai-enterprise-security-architect
2. https://www.novartis.com/about/strategy/people-and-culture
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/careers/benefits-rewards
5. https://www.novartis.com/about/strategy/people-and-culture
6. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
7. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/AI-Enterprise-Security-Architect_REQ-10074087-1
8. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/AI-Enterprise-Security-Architect_REQ-10074087-1