



Solution Architect with Cybersecurity experience | Contract

HITCONTRACT

www.hitcontract.lt

Lietuva

Apie poziciją:

Vietovė

Vilnius, Lietuva

Atlyginimas (Įrankas)

€6700 - 8700/Mėn.

Trukmė

Igalaikis projektas (>12 mėn.)

Extension (project)

Taip

Remotely (optionally)

Taip

Galioja iki

2026-08-31 (Už 4 savaites)

Aprašymas

We are part of an organisation which delivers world-class digital financial solutions to customers. We understand that change is Technology-driven and that IT is a key component for success in our journey to drive digital disruption in the bank. Our teams work with complex tech challenges and develop Danske Bank's global competitive edge on innovative digital solutions.

Responsibilities:

- Support solution architecture activities across Security GenAI Foundation initiatives, ensuring that solutions are secure, scalable, operable and aligned with Danske Bank standards.
- Translate programme objectives, solution requirements and governance expectations into concrete architecture requirements, design principles and solution patterns.
- Develop architecture artefacts such as solution designs, deployment blueprints, integration patterns, architecture decision records and security control implementation guidance.
- Help define secure-by-design patterns for AI and GenAI adoption, including identity, access, data protection, logging, monitoring, observability and runtime control requirements.
- Work with Cybersecurity Engineering, Cybersecurity Operations, enterprise

architecture, risk, compliance and technology teams to align designs across domains and influence architecture direction and ensure security is embedded before designs and solutions are finalised.

- Assess architecture options, identify risks, document trade-offs and recommend pragmatic design decisions.
- Provide guidance on integration of security tooling and controls with AI platforms, data services, cloud environments and enterprise IT services.
- Act as a sparring partner for programme teams and technical owners, helping resolve complex design questions and dependencies.
- Support architecture governance by ensuring that key decisions, assumptions, risks and design constraints are documented and communicated clearly.

Requirements:

- Broad solution architecture experience across security domains, including IAM, cloud security, data protection, infrastructure, network and platform security, monitoring, logging, defensive operations and secure integration patterns.
- Strong ability to design secure, scalable and operable solutions, including architecture blueprints, deployment designs, integration patterns, architecture decision records and control implementation guidance.
- Experience supporting strategic transformation programmes or large cross-functional initiatives with evolving scope and dependencies.
- Knowledge of AI, GenAI or machine learning security concepts, including prompt protection, model access controls, AI observability, data leakage risks, abuse cases, runtime protection or red teaming.
- Understanding of secure-by-design principles and ability to embed security controls into solution architecture from early planning stages.
- Ability to translate strategy, regulatory and governance requirements into practical architecture requirements and technical design decisions.

Senior level, + 5 years or more of experience in solution architecture, security architecture or cyber security roles, preferably within large or regulated

organisations.

Preferred start date: ASAP, 12-month assignment, with the possibility to extend.

Work location: On-Site in the Lithuania area (3-5 days On-Site, Vilnius, Lithuania).



Required Skills

REALIZACIJA

Solution Architecture 5-6 metai