



Cloud Security Architect

At If IT Security, we support our insurance business by strengthening and evolving cybersecurity capabilities across the entire organization. Our mission is to proactively identify emerging threats, implement effective controls, and ensure continuous protection of our cloud environments.

We are now looking for a Cloud Security Architect with a strong operational mindset to join our Security Operations team. In this role, you will not only design secure cloud architectures but also actively build and drive security improvements with respected platform owners. This is an ideal role for someone who enjoys hands-on technical knowledge alongside architecture responsibilities, working close to cloud team, engineering, operations, and incident response teams.

Your expertise will be focused on Microsoft Azure, but you may also work with other cloud platforms such as Google Cloud and AWS.

About the role

Translate the cloud audit policies and technical controls defined by Cloud Governance into automated, version-controlled policies (e.g., Cloud Policy, Open Policy Agent, Terraform/Bicep guardrails). Together with stakeholders ensure controls are enforced at correct scope (subscription, MG, org). Operate and continuously improve cloud security tooling such as Cloud-native security tools, e.g. Defender for Cloud. Investigate and respond to security alerts and incidents in cloud environments. Perform security hardening, vulnerability remediation, and misconfiguration fixes. Support and improve monitoring, logging, and detection capabilities (e.g., SIEM integrations). In this role you don't just maintain the baseline. Independently analyze our existing cloud security posture, identify gaps against evolving threat landscapes,

and build new automated policies to complement IT security requirements. Actively monitor, identify, and mitigate security risks and architectural drift within the Cloud Landing Zones.

Security Architecture

- Design and implement secure cloud architectures and design patterns.
- Translate architecture into deployable technical solutions (not only high-level designs).
- Build and validate proof-of-concepts and security solutions in real environments.
- Ensure security is embedded into CI/CD pipelines and DevOps workflows.

Subject Matter Expertise

- Serve as the subject matter expert (SME) on cloud security for our organization.
- Strong, hands-on experience with Microsoft Azure security ecosystems (Azure Policy, Microsoft Defender for Cloud, Azure Enterprise Landing Zones).
- Security Baseline Knowledge, familiarity with turning frameworks (like CIS Benchmarks, NIST, or internal corporate security policies) into actual runtime definitions.

Risk Assessment and Communication

- Identify, assess, and remediate cloud security risks in live environments.
- Contribute to security baselines, policies, and technical standards, with a practical, implementable approach.
- Ensure that security controls do not become developer bottlenecks. The goal is making the secure path the easiest path for product teams.
- Continuously improve security posture through measurable, operational changes.
- Work closely with IT Security, Security Engineering and Security Governance teams, IT Operations, SOC, and Engineering teams to ensure security controls are effective and operational.

About the team

Security Operations protects the organization against cyber threats through continuous monitoring, incident response, threat intelligence, and security testing. The team works proactively to detect, investigate, and respond to security threats before they impact business operations, data, or customers.

In addition, Security Operations provides infrastructure security expertise covering cloud, identity, server, network, endpoint, and Microsoft 365 environments. Through close collaboration with IT Operations and platform teams, the unit helps strengthen cyber resilience, reduce security risks, and support secure business transformation

We offer

Here are some of the benefits of working at If:

- An inclusive work environment where everyone is welcome
- Career and development opportunities in the biggest insurance company in the Nordics
- Social activities, as well as highly skilled professional environment
- Possibility of hybrid workplace
- Health promoting workplace with e.g., wellness allowance and various sports activities

- Great insurance benefits

Who are you?

You have strong hands-on experience with Microsoft Azure security services, not just designing them. In addition, you have a solid understanding of Cloud security principles, best practices, networking, containers and modern cloud architectures.

You also have:

- Experience in at least some of the following:
 - Identity and access management (Azure AD, Entra ID, PIM)
 - Cloud security monitoring and threat detection
 - Incident response and security operations
 - Security framework knowledge, like CIS or NIST
- Relevant degree in IT, Information Security, or similar field.
- Certifications such as CISSP, Azure Security Engineer, or similar are beneficial.

About the recruitment process

Application deadline: Tuesday 20.10.2026.

To apply for the position: Please attach your CV and answer the questions in the application form.

Work location: Turku, Espoo, Stockholm, Oslo or Copenhagen.

Travelling: Travelling within If countries are needed to some extend, approximately on a monthly basis.

Start: As soon as possible, to be agreed in the negotiation phase.

For more information, please contact Mika Rintamäki, Head of Security Operations +358 50 329 1855.

It is a requirement for the position that If's extended fit & proper requirements, including background checks, can be met.

If Skadeforsikring

København, 1050 København

www.if.dk

Ansøgningsfrist

20. oktober 2026

Cloud Security Architect

Kontaktperson

Mika Rintamäki

[+358 50 329 1855](tel:+358503291855)

kontakt@finansskandidaten.dk