

Lars Schiller

Senior Cloud Security Architect | DevOps Engineer | Security & Observability Engineer

Freelancer · Remote · Available from 01/2027, earlier by arrangement ·
Web: devopsdev.de · Email: lars.schiller@devopsdev.de

Professional Summary

Senior Cloud Security Architect and DevOps Engineer with more than 15 years of enterprise IT experience. Focus areas are multi-cloud security (AWS, Azure), SIEM and detection engineering, observability as code and automation with Terraform, Python and GitHub Actions. Most recently secured more than 700 cloud accounts and built monitoring and detection as code with Datadog; industry experience in financial services, energy, automotive, banking and aviation.

Core Skills

- **Cloud:** AWS, Microsoft Azure, Cloud Foundry, Landing Zones, Multi-Account Strategies, Cloud Governance, Cost Optimization
- **Security & SIEM:** Microsoft Sentinel, Datadog Cloud SIEM, Detection as Code, Sigma Rules, MITRE ATT&CK, auditd, IAM, Zero Trust, Incident Response, BAIT
- **Application Security:** Black Duck Polaris (SCA/SAST), SonarQube, Dependabot, Secret Rotation
- **Observability:** Datadog (Monitors, SLOs, Synthetic Tests, Log Pipelines), Azure Monitor, AWS CloudWatch
- **Automation & IaC:** Terraform, Bicep, ARM, CloudFormation, Ansible, API Automation (GitHub, Jira, Confluence, Datadog)
- **CI/CD & Tools:** GitHub Actions, GitHub Enterprise, Azure DevOps, Jenkins, Artifactory, Release Management, Jira Assets (CMDB), Confluence, Docker
- **Programming & Data:** Python, Java, Bash, SQL/PL-SQL, Oracle, PostgreSQL, MySQL

Professional Experience

Consultant IT Security, IT Architecture & DevOps – Leasing and mobility services provider | 06/2026 – present (planned until 12/2026)

- Observability and detection as code: Datadog monitors, SLOs, synthetic tests and security rules fully in Terraform, including a custom import tool and drift detection
- Automated conversion of Sigma rules into Datadog detection rules with MITRE ATT&CK mapping; Linux audit logging (auditd) and detection of unauthorized commands
- Automated rotation of technical Oracle DB passwords across database, GitHub secrets and Cloud Foundry, with approval gates and dry run
- GitHub migration, CODEOWNERS standard and Black Duck Polaris rollout (SCA/SAST) to more than 60 repositories
- Python automation tooling for Jira Assets (CMDB), Confluence and Cloud Foundry; release management for business-critical applications

Security Architect / Cloud Consultant – Major German energy group | 2021 – 2026

- Group-wide Cyber Defense Center for more than 700 cloud accounts (AWS & Azure) with Microsoft Sentinel as central SIEM
- Security governance, threat detection and central log management; automation with Bicep and PyTest
- Set up and operated GitHub Enterprise with GitHub Actions

Cloud / DevOps Engineer – Automotive manufacturer | 2019 – 2021

- AWS migration of an application landscape (approx. 10 TB, Oracle) with Terraform, Ansible and Jenkins; cloud cost optimization

Earlier Positions | 2009 – 2019

- **Major bank** (2016–2019): data platform for wealth management and credit assessment (Java, Oracle PL/SQL)
- **International payment services provider** (2014–2016): SEPA payments, CI/CD and release management
- **Aviation, media, telecommunications, consumer goods, energy supply** (2009–2014): Java enterprise, REST and CMS projects

Education: Diplom-Informatiker (German degree in computer science, comparable to an M.Sc.), Philipps-Universität Marburg