

Lars Schiller

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

Freiberufler · Remote · Verfügbar ab 01/2027, nach Absprache auch früher ·
Web: devopsdev.de · E-Mail: lars.schiller@devopsdev.de

Professional Summary

Senior Cloud Security Architect und DevOps Engineer mit über 15 Jahren Erfahrung in Enterprise-IT. Schwerpunkte sind Multi-Cloud-Security (AWS, Azure), SIEM und Detection Engineering, Observability as Code sowie Automatisierung mit Terraform, Python und GitHub Actions. Zuletzt Absicherung von über 700 Cloud Accounts und Aufbau von Monitoring und Detection as Code mit Datadog; Branchenerfahrung in Finanzdienstleistung, Energie, Automobil, Banking und Luftfahrt.

Core Skills

- **Cloud:** AWS, Microsoft Azure, Cloud Foundry, Landing Zones, Multi-Account-Strategien, 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-Automatisierung (GitHub, Jira, Confluence, Datadog)
- **CI/CD & Tools:** GitHub Actions, GitHub Enterprise, Azure DevOps, Jenkins, Artifactory, Release Management, Jira Assets (CMDB), Confluence, Docker
- **Programmierung & Daten:** Python, Java, Bash, SQL/PL-SQL, Oracle, PostgreSQL, MySQL

Professional Experience

Berater IT-Security, IT-Architektur & DevOps – Leasing- und Mobilitätsdienstleister | 06/2026 – heute (geplant bis 12/2026)

- Observability und Detection as Code: Datadog-Monitore, SLOs, Synthetic Tests und Security Rules vollständig in Terraform, inkl. eigenem Import-Tool und Drift-Prüfung
- Sigma-Regeln automatisch in Datadog Detection Rules mit MITRE-ATT&CK-Mapping konvertiert; Linux Audit Logging (auditd) und Erkennung unerlaubter Kommandos
- Automatisierte Rotation technischer Oracle-DB-Passwörter über Datenbank, GitHub Secrets und Cloud Foundry hinweg, mit Approval-Gates und Dry-Run
- GitHub-Migration, CODEOWNERS-Standard und Black-Duck-Polaris-Rollout (SCA/SAST) in über 60 Repositories
- Automatisierungs-Tooling in Python für Jira Assets (CMDB), Confluence und Cloud Foundry; Release-Management für unternehmenskritische Anwendungen

Security Architect / Cloud Consultant – Großer deutscher Energiekonzern | 2021 – 2026

- Konzernweites Cyber Defense Center für über 700 Cloud Accounts (AWS & Azure) mit Microsoft Sentinel als zentralem SIEM
- Security Governance, Threat Detection und zentrales Log Management; Automatisierung mit Bicep und PyTest
- Aufbau und Betrieb von GitHub Enterprise mit GitHub Actions

Cloud / DevOps Engineer – Automobilhersteller | 2019 – 2021

- AWS-Migration einer Anwendungslandschaft (ca. 10 TB, Oracle) mit Terraform, Ansible und Jenkins; Cloud Cost Optimization

Frühere Stationen | 2009 – 2019

- **Großbank** (2016–2019): Datenplattform für Wealth Management und Kreditbewertung (Java, Oracle PL/SQL)
- **Internationaler Zahlungsdienstleister** (2014–2016): SEPA-Zahlungsverkehr, CI/CD und Release Management
- **Luftfahrt, Medien, Telekommunikation, Konsumgüter, Energieversorgung** (2009–2014): Java-Enterprise-, REST- und CMS-Projekte

Ausbildung: Diplom-Informatiker, Philipps-Universität Marburg