


# Lars Schiller

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

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

Focus: Cloud, DevOps, Automation, Security

## Professional Summary

Senior Cloud Security Architect and DevOps Engineer with more than 15 years of experience designing, migrating and securing complex enterprise IT landscapes. Focus areas are multi-cloud architectures (AWS, Azure), infrastructure as code, automation and building SIEM, security and observability platforms.

Proven track record in securing large-scale cloud environments (more than 700 accounts) and establishing governance, monitoring and security standards in distributed organizations. Industry experience in financial services, energy, automotive, banking, payments and aviation.

Currently (since 06/2026) at a leasing and mobility services provider: monitoring and detection as code with Datadog and Terraform, Sigma-to-Datadog conversion with MITRE ATT&CK mapping, automated secret rotation, GitHub migration and release management for INT and PRD environments.

## Core Skills

| Area | Technologies and Methods |
|---|---|
| Cloud Platforms & Architecture | AWS, Microsoft Azure, Cloud Foundry (PaaS), Cloud Architecture Design, Landing Zones, Multi-Account Strategies, Cloud Governance, Cost Optimization, Well-Architected Framework |

| Area | Technologies and Methods |
|---|---|
| Security, SIEM & Detection Engineering | SIEM Architecture, Microsoft Sentinel, Datadog Cloud SIEM, Detection as Code, Sigma Rules, MITRE ATT&CK, Threat Detection, Security Monitoring, Linux Audit Logging (auditd), Log Management, Incident Response, SOC, IAM, Access Recertification, CSPM, Zero Trust, Vulnerability Management |
| Application Security & Compliance | SCA/SAST (Black Duck Polaris, SonarQube), Dependabot, CVE Remediation, Secret Management, Password/Secret Rotation, BAIT Reporting (German banking IT requirements), Security Governance |
| Monitoring & Observability | Datadog (Monitors, Dashboards, SLOs, Synthetic Tests, Log Pipelines), Azure Monitor, AWS CloudWatch, Availability & Capacity Management, Alerting |
| Automation & Infrastructure as Code | Process and Workflow Automation, API Automation (GitHub, Jira, Confluence, Datadog, Cloud Foundry), Self-Service and CLI Tooling, Secret Rotation, Terraform (incl. Remote State, Drift Detection, Import), Bicep, ARM Templates, CloudFormation, Ansible |
| DevOps, CI/CD & Version Control | GitHub Actions, GitHub Enterprise (Setup, Operations, Migration), Azure DevOps, Jenkins, Git, CODEOWNERS, Artifactory, Release Management |
| ITSM & Collaboration Tooling | Jira Data Center, Jira Assets (CMDB), Confluence, Change Management, Incident Management |
| Containers & Platform Engineering | Docker (hands-on experience), Kubernetes (architectural understanding), Cloud Foundry |
| Programming & Scripting | Python (CLI Tools, Automation, PyTest), Java (Enterprise Backend), Shell/Bash, SQL, PL/SQL |
| Databases & Middleware | Oracle Database, PostgreSQL, MySQL, Apache Tomcat, Oracle WebLogic |

# Professional Experience

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

- **Observability as Code:** Datadog fully managed with Terraform (remote state in S3, CI deployment, drift detection for dashboards)
- Built a custom import tool that converts existing monitors, downtimes, reference tables, security rules, suppressions and synthetic tests to Terraform (replacing the discontinued Terraformer)
- Synthetic tests generated automatically from Jira Assets (CMDB); domain monitoring, SLOs, capacity and availability dashboards and a monthly availability report for business-critical systems
- **Detection Engineering:** automated conversion of Sigma rules into Datadog detection rules including MITRE ATT&CK mapping, overrides and force-disable logic
- Extended Linux audit logging (auditd rules, deployment script) and built log pipelines that reconstruct command lines and sudo context
- Detection of unauthorized commands via a role- and environment-based allowlist in an enrichment pipeline; SIEM index cost optimization; contributions to BAIT reporting
- **AppSec:** rolled out Black Duck Polaris (SCA/SAST) via GitHub Actions to more than 60 repositories; remediated SonarQube, Dependabot and CVE findings in Python dependencies
- **Automated Secret Rotation:** rotation of technical Oracle DB passwords in a single run (database, GitHub Actions secrets, Cloud Foundry environment variables) with dry run, approval gates, parallel execution and log masking
- **GitHub Migration:** switched URLs, secrets and Artifactory integration, introduced a CODEOWNERS standard across all repositories, automated user migration and cleanup
- GitHub Actions workflow templates, an Actions dashboard on GitHub Pages and a tool for organization-wide workflow changes via pull requests
- Recertification of GitHub access with permission reports (HTML/PDF) and export of role assignments
- **Cloud Foundry:** YAML-driven role and space manager, PaaS deployment script, log drain service in all manifests
- **Automation Tooling:** Python CLIs for Jira Data Center/Jira Assets and Datadog Case Management, Confluence page generation from templates, GitHub scripts for secrets, variables, autolinks and branch cleanup

- Release management for numerous business-critical applications (ERP, BI, customer and fleet portals); code reviews, documentation, knowledge transfer and operations support

**Technologies:** Datadog, Terraform, AWS S3, GitHub Actions, GitHub Enterprise, Cloud Foundry, Python, Oracle, Jira Assets, Confluence, Artifactory, Sigma, MITRE ATT&CK, auditd, Black Duck Polaris, SonarQube

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

- Designed and built a group-wide Cyber Defense Center securing more than **700 cloud accounts (AWS & Azure)**
- Architecture, implementation and integration of a **SIEM platform based on Microsoft Sentinel**
- Design and implementation of cloud security architectures for decentralized multi-account structures
- Introduction of security monitoring, threat detection and central log management
- Established security governance and compliance standards for cloud environments
- Python-based test and validation framework (PyTest) for automated checks of account onboarding
- Automation of security and governance processes with infrastructure as code (Bicep)
- Set up and operated a GitHub Enterprise platform including organization structure, workflows and governance
- CI/CD pipelines with GitHub Actions

## Cloud / DevOps Engineer – Automotive manufacturer | 2019 – 2021

- Migrated an application landscape from on-premises to AWS
- Responsible for architecture, operations and further development of several production systems
- Managed **approx. 10 TB of data** and several Oracle databases
- Fully automated infrastructure with Terraform and Ansible
- CI/CD pipelines (Jenkins) for deployment and provisioning
- Cloud cost optimization and capacity planning
- Migration from Oracle WebLogic to Apache Tomcat

### Software Engineer / Backend Developer – Major bank | 2016 – 2019

- Central data platform for wealth management and credit assessment
- Globally used interfaces for financial systems
- Processing of large data volumes with a focus on performance, scalability and stability
- Data import, transformation and reporting processes with Oracle (SQL, PL/SQL), Java and shell

### Software Engineer – International payment services provider | 2014 – 2016

- Development and operation of systems for SEPA payments
- Batch processing with Spring Batch
- Introduced CI/CD, code reviews and release management
- Participation in incident, problem and change management
- Development of tools including an XML converter and monitoring tools

### Software Engineer – Aviation group | 2013 – 2014

- Backend for a mobile news platform (iOS/Android)
- RESTful web services, integration of the Adobe CQ5 CMS
- Java, Spring, Hibernate, Tomcat

### Further Projects (Selection) – Media, telecommunications, consumer goods, energy supply | 2009 – 2013

- Enterprise applications with Java, Spring, Hibernate
- CMS and web projects (CoreMedia, Adobe CQ5), editorial systems and web portals
- SOA, web services (SOAP/REST), relational databases

## Project Highlights

| Project | Industry | Result |
|---|---|---|
| Observability & Detection as Code | Leasing/mobility (2026) | Datadog monitors, SLOs, synthetics and security rules fully in Terraform; Sigma rules converted to Datadog automatically with MITRE ATT&CK mapping |

| Project | Industry | Result |
|---|---|---|
| Automated Secret Rotation | Leasing/mobility (2026) | Rotation of technical Oracle DB passwords including GitHub secrets and Cloud Foundry variables in a single run, with approval gates and dry run |
| GitHub Migration & AppSec Rollout | Leasing/mobility (2026) | Migration of all repositories, CODEOWNERS standard, Black Duck Polaris in more than 60 repositories |
| Cyber Defense Center | Energy (2021–2026) | Multi-cloud security platform for more than 700 AWS and Azure accounts with Microsoft Sentinel as central SIEM |
| Cloud Migration | Automotive (2019–2021) | End-to-end migration to AWS, fully automated infrastructure with Terraform and Ansible, approx. 10 TB of data |

## Education

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

Thesis: *Development of a Refactoring Plug-in for the Eclipse Modeling Framework*