

Lars Schiller

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

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

Schwerpunkte: Cloud, DevOps, Automation, Security

Professional Summary

Senior Cloud Security Architect und DevOps Engineer mit über 15 Jahren Erfahrung in Konzeption, Migration und Absicherung komplexer Enterprise-IT-Landschaften. Schwerpunkte sind Multi-Cloud-Architekturen (AWS, Azure), Infrastructure as Code, Automatisierung sowie der Aufbau von SIEM-, Security- und Observability-Plattformen.

Nachweisliche Erfahrung in der Absicherung großskaliger Cloud-Umgebungen (über 700 Accounts) und im Aufbau von Governance-, Monitoring- und Security-Standards in verteilten Organisationen. Branchenerfahrung in Finanzdienstleistung, Energie, Automobil, Banking, Zahlungsverkehr und Luftfahrt.

Aktuell (seit 06/2026) bei einem Leasing- und Mobilitätsdienstleister: Monitoring und Detection as Code mit Datadog und Terraform, Sigma-zu-Datadog-Konvertierung mit MITRE-ATT&CK-Mapping, automatisierte Secret-Rotation, GitHub-Migration und Release-Management für INT- und PRD-Umgebungen.

Core Skills

Bereich	Technologien und Methoden
Cloud Platforms & Architecture	AWS, Microsoft Azure, Cloud Foundry (PaaS), Cloud Architecture Design, Landing Zones, Multi-Account-Strategien, Cloud Governance, Cost Optimization, Well-Architected Framework

Bereich	Technologien und Methoden
Security, SIEM & Detection Engineering	SIEM-Architektur, 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, Security Governance
Monitoring & Observability	Datadog (Monitors, Dashboards, SLOs, Synthetic Tests, Log Pipelines), Azure Monitor, AWS CloudWatch, Availability & Capacity Management, Alerting
Automation & Infrastructure as Code	Prozess- und Workflow-Automatisierung, API-Automatisierung (GitHub, Jira, Confluence, Datadog, Cloud Foundry), Self-Service- und CLI-Tooling, Secret-Rotation, Terraform (inkl. Remote State, Drift Detection, Import), Bicep, ARM Templates, CloudFormation, Ansible
DevOps, CI/CD & Version Control	GitHub Actions, GitHub Enterprise (Aufbau, Betrieb, 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 (praktische Erfahrung), Kubernetes (Architekturverständnis), 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

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

- **Observability as Code:** Datadog vollständig mit Terraform verwaltet (Remote State in S3, CI-Deployment, Drift-Prüfung für Dashboards)
- Eigenes Import-Tool entwickelt, das Monitore, Downtimes, Reference Tables, Security Rules, Suppressions und Synthetic Tests nach Terraform überführt (Ersatz für den eingestellten Terraformer)
- Synthetic Tests automatisch aus Jira Assets (CMDB) erzeugt; Domain-Monitoring, SLOs, Capacity- und Availability-Dashboards sowie monatlicher Verfügbarkeitsreport für geschäftskritische Systeme
- **Detection Engineering:** automatische Konvertierung von Sigma-Regeln in Datadog Detection Rules inkl. MITRE-ATT&CK-Mapping, Overrides und Force-Disable-Logik
- Linux Audit Logging erweitert (auditd-Regeln, Deployment-Skript) und Log-Pipelines zur Rekonstruktion von CommandLine und sudo-Kontext gebaut
- Erkennung unerlaubter Kommandos über rollen- und umgebungsbasierte Whitelist mittels Enrichment-Pipeline; Kostenoptimierung des SIEM-Index; Zuarbeit zum BAIT-Reporting
- **AppSec:** Black Duck Polaris (SCA/SAST) per GitHub Actions in über 60 Repositories ausgerollt; SonarQube-, Dependabot- und CVE-Findings in Python-Abhängigkeiten behoben
- **Automatisierte Secret-Rotation:** Rotation technischer Oracle-DB-Passwörter in einem Durchlauf (Datenbank, GitHub-Actions-Secrets, Cloud-Foundry-Umgebungsvariablen) mit Dry-Run, Approval-Gates, paralleler Ausführung und Log-Maskierung
- **GitHub-Migration:** URLs, Secrets und Artifactory-Anbindung umgestellt, CODEOWNERS-Standard in allen Repositories, automatisierte User-Migration und Bereinigung
- GitHub-Actions-Workflow-Templates, Actions-Dashboard über GitHub Pages und ein Tool für organisationsweite Workflow-Änderungen per Pull Request
- Rezertifizierung der GitHub-Zugriffe mit Berechtigungsreport (HTML/PDF) und Export der Rollenzuordnungen
- **Cloud Foundry:** YAML-gesteuerter Rollen- und Space-Manager, PaaS-Deployment-Skript, Logdrain-Service in allen Manifesten
- **Automatisierungs-Tooling:** Python-CLIs für Jira Data Center/Jira Assets und Datadog Case Management, Confluence-Seitengenerierung aus Templates, GitHub-Skripte für Secrets, Variablen, Autolinks und Branch-Bereinigung

- Release-Management für zahlreiche unternehmenskritische Anwendungen (ERP, BI, Kunden- und Flottenportale); Code Reviews, Dokumentation, Wissenstransfer und Betriebsunterstützung

Technologien: 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 – Großer deutscher Energiekonzern | 2021 – 2026

- Konzeption und Aufbau eines konzernweiten Cyber Defense Centers zur Absicherung von über **700 Cloud Accounts (AWS & Azure)**
- Architektur, Implementierung und Integration einer **SIEM-Plattform auf Basis von Microsoft Sentinel**
- Design und Umsetzung von Cloud Security Architekturen für dezentrale Multi-Account-Strukturen
- Einführung von Security Monitoring, Threat Detection und zentralem Log Management
- Aufbau von Security Governance und Compliance-Standards für Cloud-Umgebungen
- Python-basiertes Test- und Validierungsframework (PyTest) zur automatisierten Prüfung der Account-Anbindung
- Automatisierung von Sicherheits- und Governance-Prozessen mit Infrastructure as Code (Bicep)
- Aufbau und Betrieb einer GitHub Enterprise Plattform inkl. Organisationsstruktur, Workflows und Governance
- CI/CD-Pipelines mit GitHub Actions

Cloud / DevOps Engineer – Automobilhersteller | 2019 – 2021

- Migration einer Anwendungslandschaft von On-Premise in die AWS Cloud
- Verantwortung für Architektur, Betrieb und Weiterentwicklung mehrerer produktiver Systeme
- Verwaltung von **ca. 10 TB Daten** und mehreren Oracle-Datenbanken
- Vollständig automatisierte Infrastruktur mit Terraform und Ansible
- CI/CD-Pipelines (Jenkins) für Deployment und Provisionierung
- Cloud Cost Optimization und Kapazitätsplanung
- Migration von Oracle WebLogic zu Apache Tomcat

Software Engineer / Backend Developer – Großbank | 2016 – 2019

- Zentrale Datenplattform für Wealth Management und Kreditbewertung
- Global genutzte Schnittstellen für Finanzsysteme
- Verarbeitung großer Datenmengen mit Fokus auf Performance, Skalierbarkeit und Stabilität
- Datenimport-, Transformations- und Reportingprozesse mit Oracle (SQL, PL/SQL), Java und Shell

Software Engineer – Internationaler Zahlungsdienstleister | 2014 – 2016

- Entwicklung und Betrieb von Systemen im SEPA-Zahlungsverkehr
- Batch-Verarbeitung mit Spring Batch
- Einführung von CI/CD, Code Reviews und Release Management
- Mitarbeit in Incident-, Problem- und Change-Management
- Entwicklung u. a. eines XML-Converters und von Monitoring-Tools

Software Engineer – Luftfahrtkonzern | 2013 – 2014

- Backend für eine mobile Nachrichtenplattform (iOS/Android)
- RESTful Web Services, Integration des CMS Adobe CQ5
- Java, Spring, Hibernate, Tomcat

Weitere Projekte (Auswahl) – Medien, Telekommunikation, Konsumgüter, Energieversorgung | 2009 – 2013

- Enterprise-Anwendungen mit Java, Spring, Hibernate
- CMS- und Webprojekte (CoreMedia, Adobe CQ5), Redaktionssysteme und Webportale
- SOA, Web Services (SOAP/REST), relationale Datenbanken

Project Highlights

Projekt	Branche	Ergebnis
Observability & Detection as Code	Leasing/Mobilität (2026)	Datadog-Monitore, SLOs, Synthetics und Security Rules vollständig in Terraform; Sigma-Regeln automatisch mit MITRE-ATT&CK-Mapping nach Datadog konvertiert

Projekt	Branche	Ergebnis
Automatisierte Secret-Rotation	Leasing/Mobilität (2026)	Rotation technischer Oracle-DB-Passwörter inkl. GitHub Secrets und Cloud-Foundry-Variablen in einem Durchlauf, mit Approval-Gates und Dry-Run
GitHub-Migration & AppSec-Rollout	Leasing/Mobilität (2026)	Migration aller Repositories, CODEOWNERS-Standard, Black Duck Polaris in über 60 Repositories
Cyber Defense Center	Energie (2021–2026)	Multi-Cloud-Security-Plattform für über 700 AWS- und Azure-Accounts mit Microsoft Sentinel als zentralem SIEM
Cloud-Migration	Automobil (2019–2021)	End-to-End-Migration nach AWS, vollautomatisierte Infrastruktur mit Terraform und Ansible, ca. 10 TB Daten

Education

Diplom-Informatiker – Philipps-Universität Marburg

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