Akhil Kulal B

Cybersecurity Engineer · Cloud Security · Compliance · AWS

Bengaluru, India +91 89710 04762 akhilbk9@gmail.com linkedin.com/in/akhil-kulal akhilkulal.in

Summary

Cybersecurity engineer with about 5 years in industry across cloud and infrastructure, now securing AWS environments at AliveCor, a digital health company. Delivers continuous cloud threat monitoring, application security testing (SAST and DAST), vulnerability remediation, and audit readiness for ISO 27001, ISO 42001 and SOC 2 Type 2. Previously a DevOps engineer, with hands-on AWS, CI/CD and automation experience that helps fixes reach production faster.

Key highlights

- Handle security incident response, from triage and containment through remediation, partnering with engineering teams.
- Rolled out generative AI from AWS Bedrock to all employees behind a VPN and built a usage and cost dashboard with weekly-budget Slack alerts.
- Deliver audit readiness across three frameworks: ISO 27001, ISO 42001 and SOC 2 Type 2.
- Conceived and co-built an automated SAST scanning tool in the CI/CD pipeline that runs on pushes to configured branches, keeps scan costs under control, and publishes findings to a central dashboard.
- Audit SaaS access and AWS and SaaS spend to reduce risk and cost.
- Cut manual deployment effort by 60% and raised uptime by 80% through earlier DevOps automation and monitoring work.

Experience

Cybersecurity Engineer · AliveCor 07/2025 – Present · Bengaluru

- Handle security incident response, from triage and containment through remediation, coordinating with engineering teams to drive each incident to closure.
- Rolled out generative AI from AWS Bedrock to all employees, with access restricted behind a VPN so prompts and company data stay on the private network.
- Built a usage and cost dashboard for the Bedrock deployment that turns token data from databases into per-user spend and sends Slack alerts when a user exceeds their weekly budget.
- Monitor the AWS environment for threats and misconfigurations using Amazon GuardDuty, Inspector, Macie, CloudTrail, CloudWatch Logs and AWS Config, with alerts routed to Slack by severity; triage findings and drive each to resolution with the owning teams.
- Conceived and co-built an automated SAST scanning tool in the CI/CD pipeline: pushes to configured branches trigger a scan only if none has run in the past 90 days, which controls per-scan cost, manual runs always scan, and results and findings are published to a central dashboard. Also run DAST scans and work with engineering to remediate vulnerabilities by priority.
- Patch cloud instances on a regular cycle to reduce exposure to known vulnerabilities.
- Moved public-facing application URLs behind Amazon CloudFront to harden how they are exposed to the internet.
- Prepare evidence, track controls and coordinate with control owners for ISO 27001, ISO 42001 and SOC 2 Type 2 audits.
- Complete customer security questionnaires, giving accurate and consistent answers on the company's security posture.

- Review user access to applications and SaaS tools and audit AWS and SaaS bills and licences, removing unused access and spend.

DevOps Engineer · Tata Consultancy Services 10/2021 – 06/2025 · Bengaluru

Client: Royal Bank of Canada

- Operated secure, highly available AWS infrastructure for a global financial services client: EC2, VPC design (subnets, route tables, NACLs, IGW, NAT) and S3 with cross-region replication.
- Enforced least-privilege access with IAM users and customer-managed policies, and enabled CloudTrail for audit and compliance.
- Set up CloudWatch monitoring with SNS alerting, and managed MySQL on RDS with backups and read replicas.
- Owned Jenkins CI/CD pipelines and the QA automation framework in Git; containerised services with Docker and managed multi-container deployments with Ansible.
- Automated deployment workflows, cutting manual effort by 60% and shortening release cycles.
- Built a real-time monitoring dashboard for application status and disk usage with downtime email alerts, improving uptime and reliability by 80%.
- Led daily stand-ups for a remote team to track progress and unblock delivery.
- Recognised with on-the-spot and steady-state operations awards for permanent fixes to recurring issues.

Skills

Security	Incident response, Amazon GuardDuty, Inspector, Macie, SAST pipeline automation, DAST, vulnerability management and patching, access reviews, security questionnaires
Compliance	ISO 27001, ISO 42001, SOC 2 Type 2
AWS	EC2, VPC, S3, IAM, EFS, RDS, Route 53, CloudFront, CloudWatch, CloudTrail, Config, Inspector, Macie, SNS
DevOps	Jenkins, Docker, Maven, Ansible, Terraform
Tools	Git, GitHub, Splunk
Scripting	Python, Shell, YAML, Declarative Pipeline
Operating systems	Linux, Windows

Certifications

- Agile Way of Working Foundation
- RDBMS Concepts
- DevOps Beginner to Advance | Decoding with Projects

Education

B.E. in Electronics and Communication Engineering
Canara Engineering College · 06/2017 – 07/2021 · GPA 7.8 / 10