

Rohit Yallaling

Hyderabad, Telangana, India | 8088080608 | rohitcloudsecops@gmail.com | <https://rohitcloudsecops.in> | LinkedIn
| GitHub

SUMMARY

Technology professional with 9+ years of experience in Platform Engineering, Platform Security, DevSecOps, Identity & Access Management (IAM), and Cloud Security across semiconductor and enterprise environments. Skilled in secure software delivery, identity governance, cloud platform support, Linux administration, and scripting using Python, Bash, and PowerShell. Passionate about leveraging AI-assisted engineering to improve productivity while delivering secure, scalable, and reliable enterprise solutions.

EDUCATION

Gulbarga University, Karnataka

Bachelor of Computer Applications (BCA)

EXPERIENCE

Senior Software Engineer

Oct 2021 – Present

AMD India Pvt. Ltd.

Domain: IAM | Cloud Security | Platform Security | DevSecOps | AI-assisted Engineering

- Supported enterprise Identity & Access Management (IAM) and Identity Governance & Administration (IGA) initiatives using SailPoint, Okta, CyberArk, and AWS IAM.
- Implemented identity lifecycle management through JML, RBAC, SSO, MFA, SAML 2.0, OAuth 2.0, OIDC, and SCIM.
- Integrated Shift Left Security practices into Secure SDLC and secure CI/CD engineering workflows.
- Strengthened cloud, platform, and container security across AWS environments using Docker, Kubernetes, and security best practices.
- Performed application, dependency, container, and Infrastructure-as-Code security validation using SonarQube, Trivy, Checkov, OWASP ZAP, Burp Suite, and Snyk.
- Developed reusable Python, Bash, and PowerShell scripts to streamline engineering workflows, improve operational efficiency, and reduce repetitive manual activities.
- Investigated production issues through debugging and root cause analysis to improve platform stability and issue resolution.
- Leveraged AI-assisted engineering to accelerate scripting, troubleshooting, documentation, and operational knowledge sharing.
- Collaborated with cloud, platform, development, and security teams to strengthen platform reliability, compliance, and security posture.
- Key Technologies: SailPoint • Okta • CyberArk • AWS IAM • Docker • Kubernetes • Python • Bash • PowerShell • Git • GitHub Actions • SonarQube • Trivy • Checkov • Burp Suite • OWASP ZAP • Snyk • Linux

Senior Software Engineer

Sep 2020 – Sep 2021

AMD India (via SpanIdea)

Domain: Platform Engineering | DevOps | DevSecOps Support

- Supported enterprise platform engineering, build management, and software release activities.
- Assisted secure CI/CD implementation and release engineering.
- Contributed to Shift Left Security through Secure SDLC and DevSecOps practices.
- Developed Python, Bash, and PowerShell scripts to simplify engineering workflows.
- Supported Linux infrastructure, deployment environments, and engineering platforms.
- Assisted security validation, compliance verification, and vulnerability assessment activities.

- Improved deployment reliability and release quality through collaboration with cross-functional engineering teams.

Senior Software Engineer

May 2019 – May 2020

Dell Technologies

Domain: Enterprise Security Application & Platform Testing

- Validated enterprise security applications across Windows platforms.
- Performed authentication, authorization, Secure Boot, TPM, and BIOS security validation.
- Executed security compliance testing, regression validation, and vulnerability verification.
- Investigated software issues through debugging and root cause analysis.
- Collaborated with engineering teams to validate security fixes and improve platform stability.

Software QA Engineer

Oct 2015 – May 2019

Toshiba Software India | Magna Infotech | Allegis Services

Domain: Graphics Driver QA | Windows Platform | Enterprise & Cloud Application Testing

- Performed graphics driver validation across Windows platforms.
- Executed Windows platform validation and enterprise/cloud application testing.
- Conducted hardware-software integration and end-to-end system testing.
- Performed debugging and root cause analysis for complex software issues.
- Collaborated with engineering teams to improve software quality and platform reliability.

PROJECTS

Enterprise Identity Governance & Access Management Platform | Built an enterprise identity governance solution automating identity lifecycle management, access governance, privileged access, and compliance workflows.

- Technologies: SailPoint • Okta • CyberArk • AWS IAM • Python • PowerShell • RBAC • JML • SCIM • OAuth 2.0 • SAML • AI-assisted Engineering
- Automated Joiner–Mover–Leaver (JML), provisioning, deprovisioning, and role management.
- Implemented RBAC, SSO, MFA, SAML, OAuth 2.0, OIDC, and SCIM.
- Built Access Review and Access Certification workflows for governance and audit readiness.
- Developed Python and PowerShell automation for identity operations.
- Integrated AI-assisted analysis for access recommendations, governance insights, and reporting.

Enterprise DevSecOps Secure CI/CD Pipeline | Designed an enterprise DevSecOps pipeline integrating security throughout the Secure Software Development Lifecycle.

- Technologies: GitHub Actions • Jenkins • Docker • Kubernetes • Terraform • SonarQube • Trivy • Checkov • OWASP ZAP • Snyk
- Implemented Shift Left Security across CI/CD pipelines.
- Integrated SonarQube, Trivy, Checkov, OWASP ZAP, and Snyk into deployment workflows.
- Automated SAST, DAST, dependency, container, and IaC security validation.
- Built Python automation for security reporting and compliance dashboards.
- Improved release quality through automated security gates.

Enterprise Cloud Security & Platform Hardening | Designed a secure cloud environment implementing identity security, platform hardening, and compliance automation.

- Technologies: AWS • IAM • CloudTrail • GuardDuty • Security Hub • Docker • Kubernetes • Terraform
- Implemented secure AWS IAM architecture using least-privilege principles.
- Configured CloudTrail, GuardDuty, and Security Hub for continuous monitoring.
- Automated infrastructure provisioning and compliance validation using Terraform.
- Strengthened Docker and Kubernetes security practices.
- Built automated cloud security monitoring and compliance reporting.

Enterprise AIOps for Cloud Security Operations | Designed an AI-assisted CloudSecOps solution to improve production operations, cloud security monitoring, and incident response.

- Technologies: AWS • CloudWatch • CloudTrail • GuardDuty • Security Hub • Docker • Kubernetes • Python • Prometheus • Grafana • AI-assisted Engineering

- Correlated cloud logs, monitoring metrics, and security alerts using AI-assisted analysis.
- Accelerated root cause analysis and operational troubleshooting.
- Generated automated cloud health reports, security insights, and remediation recommendations.
- Built intelligent dashboards for cloud security posture, operational KPIs, and production health.
- Improved production visibility through AI-assisted operational analytics.

TECHNICAL SKILLS

Identity & Access Management: IAM • IGA • SailPoint • Okta • CyberArk • AWS IAM • JML • RBAC • SSO • MFA • SAML 2.0 • OAuth 2.0 • OIDC • SCIM

Cloud Security & Platform Engineering: AWS • Platform Engineering • Platform Security • Cloud Security • Linux • Docker • Kubernetes • Terraform • Ansible

DevSecOps: DevSecOps • Shift Left Security • Secure SDLC • Secure CI/CD • Jenkins • Git • GitHub • GitHub Actions • Release Engineering

Application Security: SonarQube • Trivy • Checkov • OWASP ZAP • Burp Suite • Snyk • Vulnerability Assessment • Security Validation • Security Compliance

Programming & Scripting: Python • Bash • PowerShell • REST APIs

AI-assisted Engineering: AI-assisted Engineering • AIOps • ChatGPT • Claude AI • Cursor AI • GitHub Copilot

CERTIFICATIONS

AWS Certified Solutions Architect – Associate (Planned)

SailPoint Identity Security (Planned)

CyberArk PAM Administration (Planned)

HashiCorp Terraform Associate (Planned)

PROFESSIONAL DEVELOPMENT

Continuous learning in IAM, DevSecOps, Cloud Security, Platform Engineering, and AI-assisted Engineering.