Raj Mithun

Principle DevSecOps Engineer|Cloud Security & Platform Governance

rajmithun.m55@outlook.com
LinkedIn

Professional Summary

DevSecOps and Cloud Security Lead with ~12 years' experience building and governing secure cloud platforms across Azure, GCP and AWS in regulated financial and health-tech environments. I operate at the intersection of platform engineering and security, defining secure CI/CD standards, embedding security controls into infrastructure-as-code, and aligning cloud operations with HITRUST and ISO 27001-aligned control requirements. In my most recent role, I act as technical lead for cloud security and DevSecOps capability across multiple engineering squads, providing governance over IAM, CI/CD, infrastructure automation and monitoring standards. I focus on reducing operational risk, improving auditability, and enabling engineering teams to deliver securely at scale.

Core Skills

Cloud Security, IAM & Compliance
• Act as technical lead for DevSecOps capability across multiple product teams, defining secure CI/CD and infrastructure standards adopted across 15+ pipelines.
• Provide governance over infrastructure-as-code, IAM and cloud configurations, reviewing 100+ pull requests to ensure security, compliance and maintainability.
• Partner with security, audit and architecture teams to align cloud implementations with HITRUST and ISO 27001-aligned controls.
• Mentor engineers on secure cloud patterns, least-privilege IAM design and policy-as-code practices.
• Translate technical security risks into clear business impact and prioritised remediation plans.
• Azure AD / Entra ID, Auth0 – SAML/OIDC SSO, group-based RBAC, least-privilege access, access reviews
• Secrets management with HashiCorp Vault Enterprise; TLS 1.2+ enforcement and certificate lifecycle automation
• Designing and evaluating security controls for cloud services against HITRUST, and internal controls aligned to ISO 27001 / SOC 2
• Experience working with security controls in regulated industries (financial services and healthcare)
• Familiar with cloud security best practices and benchmarks (NIST/CIS-style controls, secure configuration baselines, defence-in-depth)

Cloud Infrastructure & Security Architectures
• Azure: hub-and-spoke networking, VMs, App Services, APIM, Private Endpoints, DR, monitoring and logging
• GCP: Vault/Jenkins platforms, networking, access controls and observability
• AWS: Linux workloads, web stacks and Kubernetes on EC2, HAProxy load-balancing
• Infrastructure as Code: Terraform / OpenTF, Terragrunt, Ansible, Packer
• Knowledge of cloud infrastructure, security architectures and standards (network security, data protection, logging/monitoring, separation of duties)

Infrastructure as Code & Platform Automation
• Advanced Terraform / OpenTofu platform engineering, module design and IaC governance
• Migration of legacy ARM-based deployments and internal tooling to Terraform/OpenTofu
• Infrastructure standardisation across multiple environments using reusable modules
• IaC pull request governance and peer reviews ensuring security, compliance and consistency
• Experience implementing scalable infrastructure patterns supporting internal product teams

Scripting, Automation & Cloud APIs
• Python (primary), C#, PowerShell, Bash – automating security checks, access changes, CI/CD and operational tasks
• Experience with JavaScript in the context of web applications / automation tooling
• Use of cloud-based APIs (Azure, GCP, AWS, Auth0, Vault, Azure DevOps) to build automated assessment and response systems
• Git, GitHub / Azure Repos, Azure DevOps, Jenkins – policy-as-code, secure CI/CD templates, approvals

Monitoring, Detection & Incident Response
• Azure Monitor, Application Insights, KQL
• Prometheus, Grafana, Nagios, Splunk for metrics, logs and alerting
• Experience reducing MTTR and improving detection through better observability and alert tuning

Collaboration, Leadership & Communication
• Presenting security risks and remediation options to technical and non-technical stakeholders (engineering, security, audit, finance, leadership)
• Mentoring engineers on secure use of cloud services, CI/CD and infrastructure-as-code
• Working across teams and regions on shared cloud security and platform initiatives

Web-Based Applications & Services
• Securing web APIs and web-services via SSO, API gateways and least-privilege service identities
• Integrating vulnerability scanning and policy checks (Snyk, TLS config, dependency scanning) into build and release pipelines

Containers & Cloud-Native Platforms
• Containerisation using Docker with optimisation and troubleshooting of Dockerfiles
• Microservices deployments using Azure Container Services
• POCs and platform experimentation using Azure Kubernetes Service (AKS)
• Container image lifecycle management using Azure Container Registry (ACR)
• Artifact management, image versioning and repository maintenance

Experience

Senior DevOps Engineer 07/2023 to 01/2026
The Craneware Group (Azure|HITRUST Compliant)

- Act as technical lead for cloud operations and cloud security on an Azure-hosted, **HITRUST**-aligned SaaS platform, defining DevSecOps standards and guiding multiple engineering squads on secure cloud adoption.
- Assess existing cloud implementations (**networking, IAM, CI/CD**), identify security issues and prioritise fixes, feeding outcomes into **Terraform/OpenTF** and **Azure DevOps templates**.

- Own **Azure AD/IAM** changes for engineering teams and integrate **Auth0 SAML/OIDC SSO** with multiple apps, including automated certificate provisioning and renewal that **reduced onboarding time by ~60%** and **lowered SSO-related incidents.**
- **Spearheaded migration from legacy ARM-template** based infrastructure provisioning and i**nternal C# tooling to Terraform/OpenTofu,** reducing infrastructure technical debt and standardising platform deployments.
- Led the **implementation of hub-and-spoke networking architecture using Terraform/OpenTofu**, improving security segmentation, scalability and routing control across multiple environments.
- **Automated RBAC provisioning** for Azure SQL users and service accounts using C#, Python and PowerShell, cutting manual access-change effort by ~85% and improving auditability for access reviews.
- **Enhanced cloud monitoring and incident response** using **Azure Monitor, Application Insights and KQL**, improving visibility of security and reliability issues and contributing to an estimated 30% reduction in MTTR.
- **Integrated Snyk** and other security checks into Azure DevOps pipelines, ensuring vulnerabilities and misconfigurations are caught early in the SDLC without slowing delivery.
- Used Azure and Auth0 APIs with Python/PowerShell to develop automated assessment and reporting scripts for licences, certificate expiries and access anomalies, replacing manual spreadsheet work and saving 12+ hours/month.
- Defined and standardised secure CI/CD patterns across 15+ Azure DevOps pipelines, introducing reusable templates, approval controls and integrated security checks to improve consistency and reduce deployment risk.
- Worked with s**ecurity, audit, analytics and finance on HITRUST-aligned IAM, TLS 1.2+,** tagging and auto-scaling; contributed evidence and technical input for HITRUST and ISO 27001–aligned control reviews.
- Provided governance over infrastructure-as-code and DevOps changes (100+ pull requests), ensuring secure design patterns, compliance alignment and long-term maintainability.
- Improved **platform observability by integrating Azure Monitor, Log Analytics Workspace and Application Insights**, enabling proactive alerting, operational dashboards and log-based security monitoring.
- Supported platform monitoring using **Site24x7** alongside Azure-native monitoring tools to detect reliability issues and infrastructure anomalies.
- Implemented automated workflows for **SQL user provisioning and RBAC access control across Azure SQL databases**, improving auditability and reducing manual access management overhead.
- Reviewed and a**pproved database change requests and queries for higher environments** while enforcing operational guardrails.
- Regularly **performed infrastructure patching**, environment maintenance and production troubleshooting across cloud environments.
- Participated in Agile ceremonies, backlog management and production support rota, **prioritising P1 incidents** and ensuring rapid issue resolution.
- **Worked closely with engineering**, security, analytics and finance teams to optimise infrastructure usage and improve **cloud cost efficiency using Azure cost management tooling**.
- Reviewed and approved 100+ DevOps/IaC pull requests, **mentoring engineers on infrastructure patterns**, CI/CD standards and secure cloud deployments

Senior DevSecOps Engineer (Cloud Infrastructure Engineer) Level 4 **06/2022 to 07/2023**

PayPal (GCP & AWS)

- **Architected and operated HashiCorp Vault Enterprise and Jenkins across GCP, AWS** as central security and CI/CD platforms for multiple global teams, **enforcing secure secrets management, TLS and RBAC across GCP and on-prem**.
- Provided architectural oversight for centralised Vault and Jenkins platforms serving multiple global teams, influencing **security standards for secrets management, TLS enforcement and RBAC models**.
- **Built highly available Vault and Jenkins clusters using Terraform, Terragrunt, Ansible and Packer**, standardising infrastructure deployments and security configurations.
- **Led migration of CI/CD systems from TeamCity to Jenkins**, implementing shared libraries, pipeline templates and scalable dynamic build agents.
- **Used Terraform, Terragrunt, Ansible and Packe**r to define secure, repeatable infrastructure and deployment patterns; regularly assessed implementations and drove remediation of misconfigurations and platform risks.
- Implemented security-critical **Jenkins pipelines (e.g. ACL IP blocking, AWS Route53/IAM/EC2 workflows)** to protect customer-facing web properties from abuse while maintaining rapid change.
- **Integrated Vault/Jenkins with Prometheus, Grafana, Nagios, Splunk and Slack** to build a full monitoring and alerting stack for access failures, abnormal activity and platform health.s
- **Developed Python and Ansible automation** to replace manual, error-prone operational tasks, reducing toil by ~11% and improving consistency of security controls.

- **Partnered with security and networking leadership** to evaluate platform risks, define mitigation strategies and prioritise remediation based on business impact.
- **Worked within PayPal's regulated financial environment**, ensuring platform changes and security controls aligned with internal compliance and risk requirements.

DevOps Engineer 06/2020 to 06/2022
Kalosbyte Systems Pvt Ltd (AWS)

- Managed 50+ Linux servers and supporting on-prem network infrastructure, with a focus on security hardening, patching and availability for client environments.
- Built CI/CD pipelines and automated deployments for web-based applications and web-services, integrating tests and basic security checks to reduce manual change risk.
- Used Ansible as configuration-as-code to define secure server builds and application configurations, reducing configuration drift and speeding patch rollouts.
- Implemented HAProxy and Apache web stacks, including deployments on Kubernetes clusters on AWS, to deliver scalable, resilient customer-facing services.
- Led maintenance windows and incident troubleshooting for critical workloads, coordinating with stakeholders and documenting remediation steps for future prevention.

BI Data Engineer & IT Infrastructure Engineer 05/2014 to 06/2020
Economy Engraveers

- Designed and maintained local and wide-area networks and 50+ on-prem servers, handling provisioning, patching (incl. SELinux), capacity and incident response.
- Owned day-to-day systems administration: account management, system documentation, performance tuning, storage allocation and OS upgrades to maintain agreed service levels.
- Implemented monitoring and alerting for business-critical processes, reducing unplanned downtime across the on-prem estate.
- In parallel, built SQL/Power BI reporting solutions on top of 100k+ record datasets, giving stakeholders insight into operations and performance.

Financial Data Engineer 02/2013 to 04/2014
Northern Trust Corp

- Worked with UK mutual fund and equity data in a highly regulated financial environment, following firm policies on data handling, access control and compliance.
- Coordinated with the IT team to resolve IAM and system-access issues impacting analysts and trading workflows.

Education

Post Graduate Diploma in Business Management
Master of Business Administration in Finance 2010 to 2012
Jain University | Pondicherry University
Modules: Business Strategy, Financial Management, Operations Management, Organizational Behaviour, IT for Managers, Data Analytics, Project Management, Risk & Compliance, Supply Chain Management.
Award: First Class (**4.0 GPA**)
Recognized for Excellence in Project Delivery and Data-Driven Decision Making.

Certifications and Achievements

- **HashiCorp** Certified Cloud Engineer: Terraform Associate 002 (2023), Vault Associate 002 (2023).
- **Edureka**: GCP Professional Engineer (2023), DevOps Engineer (2022).
- **Microsoft**: Azure DevOps Solutions AZ-400 (2022), Azure Cloud Fundamentals (2022).
- Excel to **MySQL**: Analytic Techniques for Business from DUKE University (2021).
- **Google Data Studio** (2021), IBM Certified Data Analytics (2021).
- **SQL** Essential and Advanced Training by LinkedIn (2021).
- **Toastmasters** International Certification in Communication.

REFERENCES AVAILABLE ON REQUEST