

Mansi Dinesh

Cloud Security Engineer

dineshmansi51@gmail.com | +1 (312) 889-7264 | Chicago, IL | LinkedIn

Summary

Cloud Security Engineer with 4+ years of experience securing multi-cloud environments across AWS, Azure, and Google Cloud Platform (GCP). Implemented Zero Trust Architecture, IAM controls (SAML, OIDC, OAuth, SSO, MFA), and automated SIEM/SOAR playbooks that reduced security risk and improved incident response by up to 40%. Skilled in Terraform, DevSecOps, Kubernetes, and Policy as Code (OPA), delivering scalable infrastructure aligned with SOC 2, SOX, GDPR, and ISO 27001. Strong in Python, Go, and Bash automation, networking (TCP/IP, DNS), and cross-team collaboration.

Skills

Cloud Platforms: AWS (IAM, EC2, S3, VPC, Lambda, EKS, KMS, GuardDuty, Security Hub, CloudTrail, CloudWatch), Microsoft Azure (Entra ID, Sentinel, Defender), Google Cloud Platform (GCP) (IAM, Security Command Center), Multi Cloud Security, GPU Workloads

Identity & Access Management: Zero Trust Architecture (ZTNA), RBAC, SSO, MFA, SAML, OIDC, OAuth, LDAP

Security Operations & Monitoring: Security Operations, SIEM/SOAR (Splunk, Azure Sentinel), Datadog, ELK Stack, Prometheus, Grafana, IDS/IPS, Anomaly Detection, Incident Response, Log Analytics, Forensics

Infrastructure as Code & DevOps: Terraform, CloudFormation, Ansible, Puppet, Pulumi, Policy as Code (OPA, Azure Policy), DevOps, Jenkins, GitHub Actions, GitLab CI, Docker, Containerization, Kubernetes, Helm

DevSecOps & Application Security: Secure SDLC, SAST/DAST, CI/CD Security, Container & Kubernetes Security, Vulnerability Assessment, Penetration Testing, CSPM, CNAPP

Networking & Data Protection: Networking, TCP/IP, DNS, VPC/Subnet Security, Firewalls, VPN, Microsegmentation, Encryption (KMS, SSL/TLS, AES)

Programming & Scripting: Python, Go, TypeScript, Node.js, Bash, PowerShell, SQL, REST APIs, Full Stack Development

Databases & Messaging: PostgreSQL, Redis, DynamoDB, Apache Kafka

Compliance & Governance: SOC 2, SOX, GDPR, PCI-DSS, HIPAA, NIST CSF, ISO 27001

Tools & Collaboration: Git, GitHub, GitLab, Jira, Linux, Agile/Scrum, Cross-Team Collaboration, Engineer Onboarding, Technical Communication

Professional Experience

Cloud Security Engineer, JPMorgan Chase

Jan 2025 – Present | Chicago, IL

- Architected and enforced Zero Trust (ZTNA) and granular IAM policies across AWS and Azure to secure AI/ML inference environments, reducing unauthorized access risk by 40%.
- Protected sensitive financial datasets by implementing KMS-based encryption, microsegmentation, and secure data pipelines, meeting SOC 2 and GDPR requirements.
- Embedded SAST/DAST scanning and Policy as Code (OPA) into CI/CD pipelines, improving vulnerability detection and enabling secure, compliant releases of containerized applications.
- Automated threat response by building SIEM/SOAR playbooks in Splunk and Azure Sentinel, cutting threat detection and incident response time by 35% across real-time data processing systems.
- Provisioned standardized, security-first multi-cloud infrastructure with Terraform, improving scalability and resilience for distributed engineering teams.

Cloud Security Analyst, CloudSphere IT Labs

Nov 2020 – Jul 2023 | Bengaluru, India

- Strengthened identity security by enforcing RBAC, MFA, and SSO policies across development and production environments, reducing unauthorized access risk.
- Designed secure VPC and subnet architectures with Terraform, applying network segmentation and firewall controls to isolate multi-tenant applications and protect critical data pipelines.
- Centralized logging and threat detection with AWS CloudWatch and GuardDuty, improving anomaly detection by 35% and speeding up incident investigation.
- Integrated SAST/DAST scanning of Docker containers into CI/CD pipelines, increasing vulnerability detection and securing application releases.
- Enforced encryption at rest and in transit (SSL/TLS), aligning cloud environments with SOC 2 and ISO 27001 standards.

Projects

Cloud Security Monitoring & DevSecOps Pipeline

- Engineered a secure AWS environment by configuring VPC, EC2, IAM roles, and security groups, simulating a production-grade cloud architecture with strong access controls.
- Implemented centralized logging and threat detection using CloudWatch and GuardDuty, enabling real-time monitoring and faster identification of unauthorized access and anomalies.

Secure Multi-Cloud Infrastructure with Threat Detection

- Architected and deployed a secure multi-cloud environment across AWS and Azure using Terraform, implementing VPCs, subnets, and network segmentation to isolate production and development workloads.
- Enforced Zero Trust security controls by configuring IAM roles, RBAC, and MFA, while integrating GuardDuty and Azure Sentinel for real-time threat detection and reducing incident response time.

Certificates

- Oracle Cloud Infrastructure Generative AI Professional 
- Oracle Cloud Infrastructure AI Foundations Associate 
- Oracle Cloud Infrastructure Multicloud Architect Professional 

Education

Master of Science in Computer Science, Illinois Institute of Technology

Aug 2023 – May 2025 | Chicago, IL

Bachelor of Science in Information Science, Jain University

Aug 2018 – Jun 2022 | Bengaluru, India