Varun Chandak

Pune, India | contact.varunchandak@gmail.com | linkedin.com/in/vrnchndk/ | github.com/varunchandak

Summary

Multi-cloud infrastructure expert with 10+ years of experience securing high-scale workloads across AWS, GCP, and Azure. Evolved from a deep Linux systems engineering background into architecting automated, "secure-by-default" cloud platforms. I specialize in integrating security benchmarks directly into the DevOps lifecycle through Infrastructure as Code (IaC) hardening, automated cloud governance, and platform-level threat mitigation. Proven track record of building resilient, scalable architectures that maintain rigorous security standards without sacrificing deployment velocity.

Skills

Cloud Platforms: AWS, GCP, Azure
Cloud Security: CloudCustodian, Security Hub, Security Command Center (SCC), Azure Sentinel, Defender for Cloud, DivvyCloud, CloudView, Rapid7, ELK/Elastic Stack, AI Security Governance
Endpoint & MDM: CrowdStrike Falcon, Kandji, Jamf
DevOps & IaC: Terraform, CloudFormation, GitHub Actions, Jenkins, GitLab, Docker, AI-driven DevOps Automation
Identity & SaaS: Okta, Azure AD, AWS SSO, SAML, CyberArk, Google Workspace, Microsoft 365
Scripting: Python, Bash
Leadership & Strategy: Strategic Planning, Team Leadership, Project Management, Stakeholder Engagement, JIRA, Confluence

Experience

Security Engineer - TripleLift Jun 2024 - Present
Pune, India

- Continuously matured the security program by deploying and tuning security tools and operational processes to strengthen organizational defensive posture.
- Configured and managed SIEM, EDR, and related monitoring solutions to protect servers, endpoints, and sensitive data with near real-time detection and response.
- Hardened cloud infrastructure by assessing configurations against CIS Benchmarks, closing control gaps, and improving cloud security compliance.
- Reviewed engineering and infrastructure initiatives for security control alignment, escalated identified risks through appropriate channels, and drove timely mitigations.
- Led security awareness and enablement sessions to evangelize best practices and foster a security-first culture across teams.
- Developed and maintained security procedures and operational documentation to support consistent and effective control execution.
- Drove vulnerability management and proactive threat-hunting programs to identify, prioritize, and remediate emerging threats before business impact.
- Built and maintained internal security automation using GitHub Actions, Python, and Bash to streamline security operations across cloud, identity, endpoints, and developer tooling.
- Automated AWS security compliance scorecards and recurring reporting using Security Hub and AWS Config data, publishing results to Google Sheets and Slack, saving approximately 3 to 4 hours per week.
- Implemented identity-driven access governance workflows by reconciling Okta with access platforms and enforcing approval gates and safety checks for high impact actions, eliminating common offboarding mistakes.
- Generated recurring User Access Review and permissions inventory reports for AWS and GitHub administrators, producing audit-ready exports to Google Sheets and reducing manual evidence collection time.
- Standardized severity assignment for AWS Config findings imported into Security Hub to reduce noise and ensure consistent prioritization across accounts.
- Automated endpoint inventory, monitoring, and remediation workflows for CyberArk EPM, consolidating endpoint data from multiple device sources and saving approximately 3 to 4 hours per week.
- Integrated security alert workflows into ticketing and monitoring pipelines, improving visibility, ownership, and tracking for vulnerability and security findings.

Lead DevSecOps Engineer - Ollion Feb 2016 - May 2024
Pune, India

- Directed cloud security risk mitigation across AWS, GCP, and Azure, reducing vulnerabilities by 30% through posture management and automated patching.
- Led a six-member DevSecOps team, achieving a 40% promotion rate by driving continuous learning and hands-on mentorship.

- Standardized audit and compliance procedures, supporting SOC 2 and ISO 27001 readiness and improving audit pass rates by 25%.
- Delivered 15+ SaaS migrations and cloud implementations, improving client operational efficiency by 20% through modernization roadmaps.
- Designed and implemented secure and scalable cloud infrastructure on AWS and GCP using Terraform and CloudFormation, improving reliability by 30%.
- Automated deployments and observability using Jenkins, Nagios, and New Relic, reducing deployment time by 40%.
- Optimized 10+ AWS accounts for cost efficiency and led on-premises to cloud migrations, reducing operational costs by 25%.

Systems Support Engineer - Mithi Software May 2013 - Jan 2016
Pune, India

- Improved network and server reliability by optimizing uptime, routing, and AWS instance management with focus on redundancy and availability.
- Led migration from on-premises infrastructure to AWS, improving resource utilization and cost efficiency.
- Managed high availability Linux servers supporting enterprise email services, strengthening performance and security.
- Performed regular patching and updates across multi-site Linux fleets to maintain stability and compliance.

Projects

Multi Cloud Security Governance and Compliance Engine (AWS)
- Architected an automated governance framework across 12+ AWS accounts using AWS Config and Security Hub, centralizing findings and standardizing severity normalization via OIDC authenticated workflows.
- Implemented an AI assisted reporting pipeline to summarize weekly security trends, generating executive scorecards and automated Slack notifications for account owners.
- Automated attack surface monitoring with quarterly scans for takeover exposure and dangling DNS records across all regions, improving detection coverage without manual effort.

Enterprise Identity Governance and Lifecycle Automation
- Engineered automated offboarding workflows that reconcile Okta identities with AWS IAM Identity Center and GitHub access, reducing manual errors and improving consistency.
- Developed recurring User Access Review reporting that aggregates identity and permissions data into audit ready exports, reducing manual review time by approximately 90%.
- Streamlined GitHub organization administration with automated sync plus approval gates for membership lifecycle and repository permission changes.

Automated Endpoint Security and Fleet Orchestration (CyberArk and MDM)
- Built a cross platform inventory orchestrator that unifies endpoint data from CyberArk EPM, Microsoft Intune, Kandji, and HiBob to identify coverage gaps and inconsistencies.
- Automated endpoint workflows including scheduled agent upgrades and device set organization based on device metadata, improving operational hygiene.
- Added AI assisted anomaly insights into endpoint inventory outputs and delivered actionable summaries via security Slack notifications.

Cloud Logging and SIEM Integration (Google Workspace and Rapid7)
- Designed a log streaming pipeline for Google Workspace using API subscriptions to deliver activity telemetry from 14+ applications into Rapid7 via S3.
- Automated renewal of API watch subscriptions to prevent monitoring gaps and maintain audit readiness for security investigations.

Google Cloud Foundation Landing Zone
- Led a Terraform-based project delivering scalable, secure infrastructure on Google Cloud, integrating best practices and MAS TRM taxonomy.

Migration from On Premises to Google Cloud
- Migrated infrastructure to Google Cloud using Terraform, achieving on-demand scaling, zero downtime, and improved system reliability and performance.

Streaming Service on AWS
- Migrated Asia's leading video streaming service to AWS microservices architecture, deploying containerized services with AWS ECS, Terraform, Jenkins, Docker, and Kong API, enhancing scalability and efficiency.

Video Rendering Farm on AWS
- Deployed a video rendering farm with 50+ EC2 instances using Thinkbox Deadline, Aspera, and Maya, optimized

Linux OS with Shell Scripting, and automated server provisioning for cost savings.

In-house Projects and Automation

- Automated VM patching across Azure, AWS, and GCP with Azure Arc and Update Management Center, and delivered Secure Score alerts via Defender for Cloud CSPM.
- Implemented DLP rules and security best practices in Google Workspace, migrated Atlassian tenant, and regulated cloud usage with a time-based provisioner.
- Integrated Google Workspace with AWS, Azure AD, Slack, GitHub, and Atlassian for Single Sign-On and user provisioning, contributing to ISO 27001 and SOC2 compliance.

Certifications

AWS: Security - Specialty; DevOps Engineer - Professional; SysOps Administrator - Associate; Developer - Associate; Advanced Networking - Specialty; Solutions Architect - Professional; Solutions Architect - Associate
Google Cloud: Associate Cloud Engineer; Professional Cloud Security Engineer; Professional Google Workspace Administrator
Microsoft: Security, Compliance, and Identity Fundamentals.
HashiCorp: Terraform Associate (002).

Education

Bachelor of Technology 2007 - 2011
Poornima Institute of Engineering and Technology, Jaipur, Rajasthan