DEEPAK INUGALA

Senior DevSecOps Engineer | Cloud & On-Premises Security | AI / GPU Infrastructure | International Delivery

Email: deepak.1990@hotmail.com
Phone: +971504945921
Location: Abu Dhabi, UAE
LinkedIn: linkedin.com/in/deepak-inugala

10+ yrs	6 Countries	Multi-Cloud	3,000+ Servers	Zero Trust	99.99%
DevSecOps / SRE Experience	International Delivery	Azure · AWS · G42 · Huawei	Data Center Scale	Security Architecture	Uptime Delivered

PROFESSIONAL SUMMARY

Senior DevSecOps Engineer with 10+ years of hands-on experience in cloud security, infrastructure hardening, and shift-left security practices across Azure, AWS, G42, and on-premises Kubernetes environments. Transitioning from a strong foundation as a Senior SRE/DevOps Engineer, bringing deep expertise in Azure Security Centre, Microsoft Defender for Cloud, Azure Policy, AKS security posture management, and Kubernetes-native security tooling (OPA/Gatekeeper, Falco, Trivy, Kyverno). Proven track record securing sovereign air-gapped platforms, GPU clusters, and multi-tenant Kubernetes clusters across GOVINT, OSINT, and Smart Nation verticals at G42. Experienced in embedding security into CI/CD pipelines, driving vulnerability management programs, and designing Zero-Trust architectures at enterprise scale.

TECHNICAL SKILLS

Cloud Security	Microsoft Defender for Cloud, Azure Security Centre, Azure Policy & Initiatives, Azure Blueprints, Azure Key Vault (RBAC, secrets rotation), Microsoft Sentinel SIEM, Palo Alto Firewalls, Azure Firewall, DDoS Protection, NSG/ASG hardening, AWS Security Hub, GuardDuty, IAM least-privilege, SCPs
Kubernetes Security	OPA / Gatekeeper (policy-as-code), Kyverno, Falco (runtime threat detection), Trivy (image & cluster scanning), Aqua Security, Sysdig, Pod Security Standards (PSS), NetworkPolicy enforcement, RBAC hardening, Secrets encryption at rest, Admission Controllers, cert-manager, mTLS (Istio/Linkerd), AKS security baselines, CIS Kubernetes Benchmark
DevSecOps & SSDLC	Shift-left security: SAST (Semgrep, SonarQube), DAST (OWASP ZAP), SCA (Snyk, Dependabot), IaC scanning (Checkov, tfsec, terrascan), Container image hardening, GitLab CI/CD secret scanning, SBOM generation (Syft, Grype), Pre-commit hooks, Branch protection policies
Vulnerability Mgmt	Azure Defender for Servers, Qualys, OpenVAS, CVE triage & remediation, OS patch lifecycle (Ansible), CIS Benchmark Level 2 (Linux & AKS), STRIDE threat modelling, DAST/SAST pipeline integration, post-patch compliance scanning
Identity & Access	Azure Entra ID (AAD), RBAC, PIM, Conditional Access, MFA, Managed Identities, Service Principals (least-privilege), Keycloak OIDC/SAML, OAuth 2.0 / OIDC flows, Vault (HashiCorp) dynamic secrets, cert-manager PKI
Compliance & GRC	ISO 27001, UAE IA Framework, CIS Controls, NIST CSF, SOC 2 alignment; security audit support, DR testing (RTO < 2 hrs), evidence collection for compliance reviews, Zero-Trust architecture design
Cloud Platforms	Azure (AKS, VNet, ExpressRoute, Key Vault, Defender, Sentinel, Monitor, Firewall), AWS (EKS, EC2, VPC, S3, GuardDuty, Security Hub), G42 Cloud, Huawei Cloud, OpenStack
IaC & Automation	Terraform, Ansible (CIS hardening playbooks), Helm, ArgoCD, GitLab CI/CD, GitOps, Python, Bash scripting
Observability & OS	Prometheus, Grafana, ELK Stack, Loki, Fluent Bit, Falco alerts, DCGM Exporter, Azure Monitor; Ubuntu 22.04/24.04, RHEL 8/9, CentOS, Windows Server; kernel tuning, SELinux/AppArmor, auditd

AI / GPU Infra	Enterprise GPU clusters (H100/H200/A100), MIG config, GPU Operator, DCGM Exporter, InfiniBand/NVLink, vLLM, Triton, MLflow, Kubeflow Pipelines, secure LLM serving

WORK EXPERIENCE

Senior DevSecOps Engineer | Senior SRE | DevOps | Group 42 (G42)

07/2019 – Present | Abu Dhabi, UAE | On-Site: Kazakhstan, Angola, Bahrain | Remote: Maldives, Ethiopia

Cloud Security & Azure Defender / Policy

- Managed Azure Security Centre and Microsoft Defender for Cloud across all production subscriptions — maintained Secure Score above 85%, triaged Defender alerts, and remediated critical recommendations covering compute, storage, networking, and identity layers.
- Authored and assigned 40+ Azure Policy definitions and initiatives (Deny, Audit, DeployIfNotExists) enforcing tagging, allowed SKUs, encryption-at-rest, TLS versions, diagnostic settings, and public-endpoint restrictions across GOVINT, OSINT, and Smart Nation environments.
- Configured Azure Defender for Servers (MDE integration) across 200+ VMs automated VM vulnerability assessment using Qualys built-in scanner; tracked CVE findings through Jira, applied OS and middleware patches via Ansible, achieving SLA-driven remediation within agreed windows.
- Implemented Azure Key Vault best practices: RBAC (no access-policy mode), soft-delete/purge protection, 90-day secret rotation pipelines, certificate lifecycle automation via cert-manager; integrated Key Vault references into AKS workloads using Azure AD Workload Identity.
- Deployed and tuned Microsoft Sentinel SIEM: built custom KQL detection rules, analytics rules, and playbooks (Logic Apps) for automated incident response; maintained Palo Alto and Azure Firewall rule reviews; integrated threat feeds for IOC matching.

Kubernetes & AKS Security

- Hardened AKS clusters to CIS Kubernetes Benchmark Level 2: disabled anonymous auth, enforced audit logging, enabled etcd encryption at rest, restricted API server access via authorised IP ranges, and applied Pod Security Standards (Restricted policy) cluster wide.
- Enforcing no-privileged containers, required resource limits/requests, allowed image registries (Harbor only), no hostPath mounts, required labels/annotations and network egress restrictions.
- Implemented Kyverno policies for mutating admission (auto-inject labels, default resource limits) and validating admission (block latest tags, enforce securityContext, require readOnlyRootFilesystem) across dev, staging, and production namespaces.
- Deployed Falco with custom rules for runtime threat detection: detected container escapes, unexpected outbound connections, sensitive file access, and privilege escalation attempts; routed Falco alerts to Alertmanager and PagerDuty with defined SLA response tiers.
- Integrated Trivy Operator into the cluster for continuous workload scanning surfaced CVE findings in Grafana dashboards, blocked HIGH/CRITICAL images from reaching production via admission webhook integrated with the CI/CD pipeline.
- Configured Kubernetes RBAC with principle of least-privilege: created granular ClusterRoles/Roles and bindings per team; eliminated wildcard permissions; audited service account token usage and disabled auto-mount where not required; enabled audit log streaming to Sentinel.
- Deployed cert-manager with internal Vault PKI issuer for automated TLS certificate lifecycle across 100+ services; enforced mTLS between services using Istio service mesh, providing mutual authentication and encryption-in-transit for all intra-cluster traffic.
- Managed AKS node pool OS hardening: applied CIS Ubuntu 22.04 benchmarks via custom DaemonSet; configured node image auto-upgrade with controlled maintenance windows to minimise vulnerability exposure without impacting SLAs.

DevSecOps & Shift-Left Security in CI/CD

- Embedded security gates into GitLab CI/CD pipelines: SAST (Semgrep, SonarQube), SCA (Snyk for dependency vulnerabilities), IaC scanning (Checkov for Terraform, tfsec), Dockerfile linting (Hadolint), and secret scanning — all configured as blocking stages for production deployments.
- Implemented container image hardening standards: multi-stage Dockerfiles, distroless/scratch base images, non-root user enforcement, read-only filesystem, dropped Linux capabilities; scanned all images with Trivy before push to Harbor internal registry.
- Generated SBOMs (Software Bill of Materials) using Syft and Grype for all production container images; maintained artefact provenance with Cosign image signing — verified signatures at admission via OPA policy before deployment.

- Built automated patch pipelines in Ansible for OS vulnerability remediation (Ubuntu 22.04/24.04, RHEL 8/9): CVE triage from Defender/Qualys feeds, tested patch rollout in staging, promoted to production with automatic rollback on health-check failure.

Compliance, Zero-Trust & Governance

- Designed Zero-Trust network architecture for sovereign air-gapped environments: micro-segmented Kubernetes NetworkPolicies, Palo Alto east-west inspection, just-in-time (JIT) VM access, Azure AD Conditional Access with MFA for all privileged access, and Privileged Identity Management (PIM) for Azure RBAC elevation.
- Led annual DR testing achieving RTO under 2 hours; implemented Velero for Kubernetes backup and Longhorn snapshot replication to MinIO; documented RPO/RTO objectives and conducted tabletop exercises with client security teams.
- Supported ISO 27001 and UAE IA Framework compliance: produced evidence packs, mapped controls to Defender recommendations, authored security runbooks and incident response playbooks; liaised with client CISOs during audits across Kazakhstan, Angola, and Bahrain.
- Conducted STRIDE threat modelling workshops for new platform features; maintained risk registers and tracked remediation; produced security architecture review documents for GOVINT and Smart Nation projects.

AI / GPU Infrastructure Security

- Secured enterprise GPU clusters (H100/H200/A100): network-isolated GPU node pools with dedicated NSGs, restricted InfiniBand fabric access, RBAC-controlled MIG profile assignment, and Falco rules for GPU workload anomaly detection.
- Hardened vLLM-based LLM serving stacks: API authentication via LiteLLM gateway (API key enforcement), TLS termination at nginx reverse proxy, Kubernetes NetworkPolicy restricting model service ingress and audit logging of all inference requests via Fluent Bit to ELK.

International Delivery — On-Site & Remote (6 Countries)

- Deployed and commissioned G42 platforms (GOVINT, OSINT, Smart Nation) at client sites across Kazakhstan, Angola, and Bahrain — acted as sole technical authority for infrastructure, security, and SRE; supported Maldives and Ethiopia remotely.
- Led client security onboarding and training: delivered knowledge-transfer workshops on platform security posture, runbook handover, SLA documentation, and escalation paths with embedded security controls.

Cloud Engineer | First Abu Dhabi Bank (FAB)

02/2018 – 07/2019 | Abu Dhabi, UAE

- Completed FGB-NBAD bank merger IT integration with zero major security incidents; enforced AWS IAM least-privilege policies, Security Group hygiene, and CloudTrail audit logging across merged environments.
- Owned full vulnerability management lifecycle: triaged CVEs by severity, applied OS and middleware patches via Ansible, validated remediation through post-patch scanning — reduced repeat incidents by 35%.
- Designed and managed highly available AWS architectures (EKS, EC2, RDS, S3, Lambda) with AWS Well-Architected Framework security pillar reviews; centralised monitoring via CloudWatch, Prometheus, and Grafana.
- Deployed and managed multi-node Elasticsearch clusters with Kerberos and Ranger RBAC for secure data access in Cloudera CDH (HDFS NameNode HA, YARN, Hive, HBase, Spark, Zookeeper).

Linux Engineer | HCL InfoSystems Limited

04/2015 – 01/2018 | Abu Dhabi, UAE

- Managed large-scale Linux fleet (RHEL, CentOS, 3,000+ physical servers): OS hardening, Ansible configuration management, performance tuning, hardware fault diagnosis (iDRAC/iLO), and firmware lifecycle across Dell, HP, IBM servers.
- Configured and managed Cisco/IBM network switches (VLAN, trunk/access, STP/RSTP, LACP port-channels); administered firewall rule sets — DMZ segmentation, NAT, ingress/egress access controls.
- Led on-premises-to-cloud migration of Linux infrastructure and Cloudera Hadoop clusters with under 2 hours downtime and 0% data loss; managed full project delivery including timeline, budget, and stakeholder communication.

CERTIFICATIONS

Microsoft Certified: Azure Administrator Associate (AZ-104) *Valid: 02/2026 – 07/2027*	**Microsoft Certified: Azure Solutions Architect Expert (AZ-305)** *Valid: 07/2025 – 07/2027*
AWS Certified Solutions Architect – Associate *Valid: 07/2022 – 07/2025 | ID: PFR7HTQ25EFQQS9T*	**Certified Kubernetes Administrator (CKA)** *Valid: 09/2021 – 09/2023 | Renewal in Progress*
G42 Cloud Certified Engineer *Valid: 10/2021 – 12/2024 | ID: G42C/SVD/CRT/0475*	**Red Hat Certified Engineer (RHCE)** *Valid: 02/2015 – 02/2018 | ID: 150-012-904*
Target: Microsoft SC-100 (Cybersecurity Architect Expert) *Planned — aligns with DevSecOps architect track*	**Target: CKS – Certified Kubernetes Security Specialist** *Planned — in active preparation*

EDUCATION

Master of Business Administration (MBA) *Jawaharlal Nehru Technology University | 2012 – 2015*	**Bachelor of Technology (B.Tech)** *Jawaharlal Nehru Technology University | 2008 – 2012*

LANGUAGES & SOFT SKILLS

Languages English & Hindi (Professional) | Telugu (Native) | German (Elementary)	**Soft Skills** Security-First Mindset | Cross-functional Collaboration | Stakeholder Communication | Rapid Learning | Adaptability