# GADDIPATI **LOHIT**

lohitgaddipati@gmail.com | (425)-494-9600 | LinkedIn | Portfolio | GitHub | GitLab | Docs

## Skills & Technologies

**Cloud Platforms** : Azure, AWS and GCP.
**Infra as Code** : Terraform, Cloud CLI, Bicep, Cloud Formation, Crossplane, Ansible, Packer.
**Programming** : Python, Go, Bash, SQL, Azure SDK, AWS SDK.
**Security Tools** : Wiz, Microsoft Sentinel, Defender for Cloud, Splunk, Wireshark, tcpdump.
**DevOps & CI/CD** : GitLab, GitOps, Argo CD, Flux, Docker, Kubernetes.
**Identity & Access** : Entra AD, Active Directory, AWS IAM, AWS Identity Center, SAML SSO, MFA, Conditional Access
**OS & Networking** : Linux, Network Reconnaissance, Server Hardening
**Observability** : Prometheus, Grafana, Kubernetes, ELK, RDS Monitoring
**Security Practices**: IAM, OAuth, SCIM, Federated Authentication, Threat Detection, Incident Response, Patching, SIEM, Compliance (CIS, NIST, SOX), Cost Optimization, Log Analysis, Secure SDLC, Security controls & Framework like TLS, Zero-trust, Vulnerability assessment, Adaptable.

## Professional Experience

### Cloud Security Engineer
Bothell, WA
*Lead Engineer, T-Mobile*
present

• **Centralized Identity Management**: Engineered a solution across AWS and Azure using Azure PIM and SAML federation with IAM Identity Center, enabling Just-In-Time access and reducing over-provisioned roles by 40%.
• **SIEM Implementation & Alert Tuning**: Deployed and tuned Microsoft Sentinel to collect logs across AWS, Azure, and GCP; triaged 1000+ alerts and implemented automations that reduced false positives by over 55%.
• **Custom Sentinel Alerts & Playbooks**: Created KQL-based detection rules and integrated playbooks for automated response actions like user isolation, IP blocking. Improved MTTR by automating 60% of triage tasks.
• **Patch Compliance Framework:** Developed a scalable solution that scans for software inventory compares against a baseline and generates compliance reports for auditors. Enhanced visibility into patch SLAs across business units.
• **Zero-Day Patching Automation**: Leveraged Azure SDK for Go and GitLab to create an on-demand patching solution triggered manually during critical vulnerabilities. Used Azure Update Manager and maintenance configurations to apply updates within defined patch windows.
• **Developer Platform (Terraform & Crossplane):** Built secure infrastructure provisioning pipelines using Terraform and Crossplane with GitOps via Argo CD and Flux.
• **Golden Image Hardening:** Created hardened base images using Packer for AWS and Azure VMs, integrating endpoint agents, audit controls, and CIS-aligned configurations to ensure baseline security.
• **Wiz Monitoring & Remediation:** Monitored cloud environments with Wiz for misconfigurations, exposed secrets. Automated remediation actions via GitLab CI/CD pipelines, achieving 95% SLA adherence for high-severity issues.
• **Containerized Microservices Deployment:** Containerized microservice applications written in Go, Python, Rust, and Java along with deploying them to Kubernetes with RBAC for HA and Fault Tolerance.
• **Security Dashboards:** Built Grafana dashboards with Prometheus data sources to visualize patch status, IAM risk exposure, Sentinel alert trends, and compliance across cloud workloads.
• **Cloud Security Automation:** Wrote reusable Go and Python scripts using AWS and Azure SDKs to automate identity validation and misconfiguration checks. Fully integrated with GitLab for CI/CD enforcement.
• **Incident Analysis:** Correlated alerts in Microsoft Sentinel to investigate suspicious activity with raw logs from ADX clusters and Log Analytics workspaces, increasing overall security posture by 15%
• **SSO and MFA Configuration:** Integrated Azure AD with SAML and enforced MFA across cloud apps, aligning with audit requirements.

### University at Buffalo
Buffalo, NY
*Cybersecurity Program*
2023

**Azure Identity & Access Management:**
**-** Configured federated Single Sign-On (SSO) using SAML and integrated MFA and Self-Service Password Reset (SSPR) in Azure AD to enhance identity security and streamline access control.
**Microsoft Sentinel Deployment**
- Set up Microsoft Sentinel for log ingestion and threat detection. Built custom analytic rules and automation workflows to triage alerts and build incident response dashboards.
**Terraform-based AWS Lab**
- Created a secure development environment in AWS using Terraform, including VPC, route tables, subnets, and internet/NAT gateways.
**Vulnerability Testing Lab**
- Built a purposely vulnerable web app to test and remediate SQL injection attacks, simulating real-world attack/defense scenarios.
**Azure Firewall Implementation**
- Deployed Azure Standard Firewall with full NAT, application/network rules, and threat intelligence mode to harden the perimeter against external threats.

**Server Hardening and vulnerability management**
- Championed server hardening and vulnerability management, significantly reducing potential breach exposure by 85%. This strategic intervention fortified defenses and enhanced data protection.

**Network Reconnaissance & Packet Analysis**
- Detected brute-force login attempts and used packet inspection tools to assess lateral movement and command reconnaissance attempts.

### Cloud Security Engineer
DocSite

*Home lab and Personal Initiative* 2021

• **Containerizing Microservices on AWS**: Dockerized open-source e-commerce microservices and deployed them on AWS with Terraform and GitLab CI/CD, streamlining the release pipeline.
• **Crossplane GitOps with Argo CD**: Deployed infrastructure using Crossplane managed through Argo CD for GitOps-based IaC in a Kubernetes environment
• **K3s Cluster with Dashboard Monitoring**: Built a lightweight Kubernetes cluster using K3s, installed Kubernetes Dashboard, and configured Prometheus/Grafana for monitoring.
• **Self-Signed TLS for Kubernetes with Traefik and Cert Manager:** Secured internal traffic using self-signed certs managed by Cert Manager and Traefik as ingress.
• **AWS Account Creation & Azure SAML Integration:** Automated new AWS account setup and integrated it with Entra ID (Azure AD) for federated SSO and centralized access.
•**SQL Injection Testing Lab:** Developed and secured a vulnerable web app to simulate and patch SQLi exploits.

### Security Analyst Intern
Chennai, India

*K7 Computing* 2021

• Implemented and tested pfSense firewall configurations in lab environments, leading to a 30% reduction in exposure during vulnerability scans.
• Rebuilt and optimized internal firewall architecture to improve rule visibility and threat filtering effectiveness.
• Simulated internal attacks and improved detection capabilities in virtualized testbeds.

## Certifications

Google Cybersecurity Professional Certificate 2023