PRASANTH PANNEER SELVAM

Bengaluru, India | +91 9361571318 | prasanthp.080902@gmail.com

linkedin.com/in/prasanthpanneer | github.com/Prasanth0809 | prasanth-portfolio-blond.vercel.app

PROFESSIONAL SUMMARY

Azure Administrator with hands-on experience building and securing enterprise-grade Microsoft Azure environments. Proven ability to architect secure Virtual Networks, enforce least-privilege access with custom RBAC roles, implement centralized monitoring pipelines using Log Analytics and KQL, automate governance with Azure Policy, and manage security posture with Microsoft Defender for Cloud — aligned with real-world Azure Administrator responsibilities.

TECHNICAL SKILLS

Microsoft Azure:	Resource Groups, Virtual Networks (VNet), Subnets, NSG, RBAC, Custom RBAC Roles, Log Analytics Workspace, Diagnostic Settings, Azure Monitor, Alert Rules, Action Groups, Azure Policy, Microsoft Defender for Cloud, Storage Accounts
Security & Governance:	Least Privilege, IAM, Custom Role Definitions, IP Whitelisting (/32 CIDR), SSH Hardening, Network Isolation, Private Endpoints, Encryption at Rest, Azure Policy Enforcement, Resource Tagging
Monitoring & Logging:	KQL (Kusto Query Language), Activity Log Investigation, AzureDiagnostics, Alert Rules, Action Groups, Log Ingestion Pipelines, Security Event Detection, Failed Operation Monitoring
Cloud Concepts:	Secure Cloud Architecture, Network Segmentation, Attack Surface Reduction, Defense in Depth, Centralized Monitoring, Incident Detection & Response, Cloud Governance
Tools:	Azure Portal, Git, GitHub, Microsoft Defender for Cloud, Azure Cost Management

CERTIFICATIONS

- Microsoft Certified: Azure Fundamentals (AZ-900) – Microsoft
- AWS Cloud Quest: Cloud Practitioner – Amazon Web Services
- AWS Cloud Practitioner Essentials – Amazon Web Services

PROJECTS

CloudGuard – Enterprise Azure Secure Cloud Infrastructure

Jan 2026 – Mar 2026

github.com/Prasanth0809/azure-secure-cloud-infrastructure

- Architected a secure Azure environment using dedicated Resource Groups and a structured Virtual Network (10.0.0.0/16) with isolated public (10.0.1.0/24) and private (10.0.2.0/24) subnets, eliminating flat network exposure.
- Reduced attack surface by 100% on sensitive subnets by implementing custom NSG inbound rules restricting SSH access to a single trusted IP (/32 CIDR), preventing unauthorized administrative access.
- Built a centralized security monitoring pipeline by configuring Activity Log Diagnostic Settings to stream administrative, security, and policy events into a dedicated Log Analytics Workspace — enabling real-time subscription-wide visibility.
- Wrote and executed 3 KQL security investigation queries detecting resource write operations, administrative events, and failed operations — validating zero failed events during the monitoring period.
- Reduced incident mean-time-to-detect (MTTD) by configuring Azure Monitor Alert Rules targeting administrative error events with automated email notifications via Action Groups, completing the full detection-to-response pipeline.
- Enforced least-privilege access by designing a custom RBAC role (phase5-monitor-reader) scoped at subscription level with read-only permissions, eliminating all standing admin privileges across the environment.
- Automated governance compliance by assigning Azure Policy (Require a tag on resources) at subscription scope, enforcing mandatory Environment tagging and reducing untagged resource risk to zero.
- Improved security posture by reviewing Microsoft Defender for Cloud Secure Score, investigating recommendations, and mapping controls against the Azure Security Benchmark compliance framework.

EDUCATION

Post Graduate Diploma – Cloud Data Management

Jan 2024 – Apr 2025

Conestoga College, Kitchener, Ontario, Canada | GPA: 3.34/4.0

B.E – Computer Science & Engineering

Aug 2019 – Apr 2023

Kumaraguru College of Technology, Coimbatore, India | CGPA: 8.06/10