Neel Moradiya

347-302-5277 | neelmoradiya08@gmail.com | linkedin.com/in/moradiya-neel | github.com/moradiya-neel | neelmoradiya.com

Technical Skills

Cloud Security : AWS IAM, IAM Identity Center, Organizations & SCPs, VPC, KMS, Secrets Manager, AWS WAF
Monitoring & Detection : CloudTrail, CloudWatch, GuardDuty, Security Hub, AWS Config, Inspector, Flow Logs
AWS Services : EC2, S3, RDS, Lambda, CloudFront, ALB, Route 53, ACM, Systems Manager, AWS Backup
Threat Hunting & Vulnerability : Microsoft Defender for Endpoint, KQL, Azure Log Analytics, Tenable (Nessus)
Automation & Systems : Python, Terraform, PowerShell, Windows, Windows Server, Linux, Active Directory, Azure
Frameworks : MITRE ATT&CK, NIST CSF, CIS Benchmarks, OWASP Top 10, CVE/CWE, CVSS
Certifications : CompTIA Security+, AWS Certified Cloud Practitioner

Experience

Independent Contractor, Confidential Healthcare Client Mar 2026 – Present
AWS Cloud Security Engineer (Contract) *New York, NY*

- Design and maintain AWS security controls for a healthcare client across IAM, networking, and encryption.
- Enforce least-privilege IAM, separation of duties, and scoped permissions to fix over-permissioned access.
- Run detective controls using CloudTrail, CloudWatch alarms, GuardDuty, Security Hub, and AWS Config.
- Review AWS resources for public exposure, weak permissions, and misconfigurations, then remediate them.
- Found guessable passwords and no MFA across the environment and addressed both after supervisor approval.
- Secure the on-site server, network equipment, and firewall, and upgraded Windows PCs after Windows 10 EOL.
- Assess infrastructure changes for security risk and maintain architecture diagrams and recovery runbooks.

Diversity Infotech Dec 2022 – Dec 2023
Cloud Engineer *Surat, India*

- Built 7+ AWS VPC architectures from scratch with private subnets, NAT, and security groups; helped on 12+.
- Supported 200+ EC2 workloads with load balancing, scaling, monitoring, and recovery for 12+ SMB clients.
- Automated EC2 workload deployments with Terraform and scripted a few other cloud tasks with Python.
- Managed IAM and security controls across S3, RDS, and AWS Organizations for clients with 30+ users each.
- Used CloudWatch and CloudTrail for operational visibility, logging, troubleshooting, and investigation.
- Reviewed utilization and recommended cost and security changes that cut client AWS spend by about 8%.

Diversity Infotech Sep 2022 – Nov 2022
Cloud Infrastructure Intern *Surat, India*

- Supported cloud deployment, user access, and monitoring, and troubleshot connectivity and permissions.

Projects

SecureCart - AWS Security Architecture Redesign | *AWS VPC, ALB, EC2, RDS, S3, AWS WAF, KMS*

- Rebuilt an exposed e-commerce app (public EC2, open SSH, public RDS) as a custom VPC with private subnets.
- Chained security groups so the app accepted only ALB traffic and RDS only app traffic, with a /32 bastion.
- Enabled RDS encryption, S3 Block Public Access, SSE-S3, and AWS WAF rules that blocked SQL injection.

Vulnerability Management Program | *Tenable, PowerShell, Azure, Active Directory*

- Ran credentialed Tenable scans on an Azure Windows Server and cut findings 80% (30 to 6), criticals to 0.
- Drafted the policy, ranked fixes by risk, applied PowerShell remediations, and wrote a risk acceptance.

Threat Hunt - Azuki Breach Saga | *Defender for Endpoint, KQL, Log Analytics, MITRE ATT&CK*

- Investigated 91 flags of a simulated 8-day ransomware attack with KQL in Defender for Endpoint and Azure.
- Traced the attack across 5 systems and 6 accounts, mapped 27 MITRE ATT&CK techniques, and advised fixes.

Education

Master of Science in Cybersecurity, GPA 3.7/4.0 New York, NY
Yeshiva University *Jan 2024 – Dec 2025*

- **Relevant Coursework**: Cloud Computing, Cloud Security, Network and Data Security, Digital Forensics.