Kiran Regmi

Dallas, TX | 254-730-0635 | kiranimani@gmail.com | www.kiranregmi.com

PROFESSIONAL SUMMARY

Entry-level SOC Analyst with hands-on experience in alert triage, log analysis, phishing detection, and identity-related investigations through practical labs and production-like environments. Strong foundation in SIEM monitoring, IAM, cloud platforms, and security documentation. Brings a GRC-informed, process-driven approach to investigations, escalation, and incident reporting. Prepared to contribute effectively in a Tier-1 SOC environment.

CORE SOC SKILLS

- SIEM Monitoring & Alert Triage (Splunk)
- Incident Investigation & Escalation
- Phishing Analysis & Email Threat Detection
- Authentication & Access Event Analysis
- Vulnerability Context & Risk Prioritization
- IAM & Least-Privilege (AWS, AD concepts)
- Incident Documentation & Case Notes

SECURITY TOOLS & TECHNOLOGIES

- Networking – Routers, Switches, Firewalls, TCP/IP, OSI, DNS, DHCP
- SIEM – Splunk, Microsoft Sentinel
- Cloud – AWS (EC2, IAM, VPC), Microsoft Azure
- Operating System – Windows, Linux (Red Hat)
- Workflow – Jira, ServiceNow (exposure), Git/GitHub

SECURITY PROJECTS (SOC-RELEVANT)

- Investigated phishing simulations to identify credential-harvesting attempts and documented findings for escalation
- Designed vulnerability lifecycle: detection -> prioritization -> remediation tracking
- Analyzed authentication and access events to identify excessive permissions and enforce least-privilege alignment

(Full investigation details available at www.kiranregmi.com)

PROFESSIONAL EXPERIENCE

Owner & Operations Manager | JKM LLC | 2021 – 2025

- Investigated and resolved access, system, and payment related security issues
- Monitored operational systems for anomalies and documented incidents
- Implemented security controls aligned with FISMA Low/Moderate-style principles
- Created SOPs to serve as a knowledge base for system setup and compliance
- Managed user access and enforced least-privilege across POS and internal systems

Impact: Reduced food waste from 10% to 1% and transitioned legacy POS into a tech-enabled kitchen system, improving operational efficiency

DevOps Engineer (Contract) | NextEra Energy | 2020 – 2021

- Supported IAM provisioning and access troubleshooting across AWS and Bitbucket
- Performed access review aligned with NIST AC controls (AC-2, AC-3)
- Assisted in investigating authentication and permission-related issues
- Documented findings and supported escalation for cloud security concerns

Impact: Contributed to the successful rollout of ServiceNow Project integration.

Project Manager (Contract) | One Stops Creates | 2019 – 2019

- Managed IT/web projects, including onboarding clients and troubleshooting technical issues
- Assisted clients in resolving WordPress/MySQL environment issues, and reducing daily support tickets by 25%

Impact: Reduced owner's admin workload by 4+ hours per day through process optimization

EDUCATION

- Cybersecurity / Desktop Support Technician (Instructor Lead Program) – Computerminds.com
- miniMBA Certificate – University of Omaha, Omaha, NE
- BS, Management – Bellevue University, Bellevue, NE
- Associate of Science – Kathmandu, Nepal

CERTIFICATIONS

- CompTIA Security+
- Cisco CCST: Networking
- Microsoft Azure | Security & Identity | 365
- ISC2 NIST Cybersecurity 2.0