KIRAN REGMI

DFW, TX | US Citizen | 254-730-0635 | kiranimani@gmail.com | kiranregmi.com

PROFESSIONAL SUMMARY

Dynamic entry-level SOC Analyst with hands-on experience in SIEM and EDR platforms such as Splunk, QRadar and CrowdStrike, specializing in alert triage, incident investigation, and threat intelligence analysis. Currently focused on developing secure web applications utilizing JWT/OAuth authentication and creating AI-powered automation agents. Combines strong technical investigation skills with secure development practices, GRC-informed decision-making, and AI-enhanced workflows, ready to make an immediate impact in a Tier-1 SOC environment.

SKILLS & TOOLS

- **SIEM Monitoring & Alert Triage:** Splunk, IBM QRadar, CrowdStrike
- **Threat Intelligence & IOC Research:** VirusTotal, Cisco Talos Intelligence, Shodan, AbuseIPDB
- **Incident Response & Documentation:** Jira, ServiceNow, Case Management, Root Cause Analysis
- **Development & Security:** Node.js, JavaScript, CSS, JWT, OAuth, Vercel, Render, Git/GitHub
- **Cloud Platforms & IAM:** AWS (EC2, IAM, VPC), Microsoft Azure
- **Compliance Frameworks:** NIST, FISMA, Security Auditing
- **Networking:** TCP/IP, DNS, DHCP, Firewalls, OSI Model
- **AI & Automation:** n8n workflow automation, AI agent development (voice agents, job search, recruiter screening)

SOC ANALYST TRAINING

Cydeo SOC Analyst Program | In Progress

- Investigated directory traversal attack (decoded /cgi-bin/.%2e/.%2e/bin/sh), validated IOCs via VirusTotal/Talos/Shodan/AbuseIPDB
- Built SPL queries in Splunk for threat hunting; utilized QRadar for event correlation and security monitoring
- Triaged alerts, performed log correlation, created incident documentation in Jira following SOC procedures
- Investigated phishing simulations and analyzed authentication events to enforce least-privilege access controls

PROFESSIONAL EXPERIENCE

Founder & Security Analyst | kiranregmi.com | Jan 2026 – Present

- Architected secure web app (Node.js, Vercel/Render) with JWT/OAuth authentication; conducted internal security audit
- Built AI voice agent (n8n) for cybersecurity Q&A; developed automation for job search monitoring and recruiter screening
- Developing monitoring/logging capabilities for security event detection and incident response

Key Projects: SOC Analyst Interview Mastery, AI Agent Development tutorials, Kids' Learning Platform

Owner & Operations Manager | JKM LLC | 2021 – 2025

- Investigated access control and payment security incidents; implemented FISMA Low/Moderate controls, managed IAM provisioning
- Developed SOPs for secure system configuration and compliance documentation

Impact: Reduced operational waste by 90% through tech-enabled improvements

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

- Supported IAM provisioning/access reviews across AWS and Bitbucket; performed NIST AC control audits (AC-2, AC-3)
- Investigated authentication failures and documented security findings for escalation; improved IAM security posture

EDUCATION

BS, Management – Bellevue University | miniMBA Certificate – University of Omaha

CERTIFICATIONS

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

My AI assistant is available: ☎ *Call (254)433-4635 for quick answers*