KIRAN REGMI

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

PROFESSIONAL SUMMARY

Entry-level SOC Analyst with hands-on experience in SIEM platforms (Splunk, QRadar), alert triage, incident investigation, and threat intelligence analysis. Currently developing secure web applications with JWT/OAuth authentication while building AI-powered automation agents. Proven ability to detect and investigate security incidents including directory traversal attacks, phishing campaigns, and authentication anomalies. Combines technical investigation skills with secure development practices, GRC-informed decision-making, and AI-enhanced workflows. Ready to contribute immediately to a Tier-1 SOC environment.

CORE SOC COMPETENCIES

- SIEM Monitoring & Alert Triage (Splunk, QRadar)
- Incident Investigation & Root Cause Analysis
- Threat Intelligence & IOC Research
- Log Analysis & Event Correlation
- Vulnerability Assessment & Security Auditing
- Security Incident Documentation & Escalation
- AI Agent Development & Security Automation

SECURITY TOOLS & TECHNOLOGIES

SIEM & Detection: Splunk, IBM QRadar, Microsoft Sentinel
Threat Intelligence: VirusTotal, Cisco Talos Intelligence, Shodan, AbuseIPDB
Development & Security: Node.js, JavaScript, CSS, JWT, OAuth, Vercel, Render
Cloud Platforms: AWS (EC2, IAM, VPC), Microsoft Azure
Networking: TCP/IP, DNS, DHCP, Firewalls, OSI Model
Operating Systems: Windows, Linux (Red Hat)
Ticketing & Workflow: Jira, ServiceNow, Git/GitHub
AI & Automation: n8n workflow automation, AI agent development (voice agents, job search, recruiter screening)

RELEVANT TRAINING & PROJECTS

SOC Analyst Training Program | Cydeo | In Progress

Hands-on production-like SOC training with real-world incident investigation and SIEM operations

Key Investigations & Detections:

- Directory Traversal Attack Investigation: Detected and analyzed web server exploitation attempt using encoded path traversal technique (/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh decoded to /cgi-bin/../../../../../../../../../../bin/sh) with suspicious user agent "libredtail-http" from IP 156.245.248.226
- Conducted multi-source threat intelligence research using VirusTotal, Talos Intelligence, Shodan, and AbuseIPDB to validate IOCs and assess threat actor patterns
- Performed log correlation across multiple data sources to identify attack patterns and establish incident timelines
- Triaged and prioritized security alerts based on severity, asset criticality, and potential business impact
- Created detailed incident documentation and case notes in Jira ticketing system following SOC procedures

Technical Skills Developed:

- Built and executed SPL queries in Splunk for threat hunting and alert investigation
- Utilized QRadar for event correlation and security monitoring
- Analyzed authentication logs, web server logs, and network traffic for anomalous behavior
- Validated and enriched security alerts with external threat intelligence sources

Additional Security Projects:

- Investigated phishing simulations to identify credential-harvesting attempts and social engineering techniques, documented findings with recommended containment actions
- Designed vulnerability lifecycle workflow and analyzed authentication events to enforce least-privilege access controls

PROFESSIONAL EXPERIENCE

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

Developing cybersecurity learning platform and AI-powered automation solutions with focus on secure development practices and operational security

- Architected and deployed secure web application using Node.js, JavaScript, and CSS hosted on Vercel (frontend) and Render (backend)
- Implemented JWT and OAuth authentication mechanisms to secure user access and protect learning portal content
- Conducted internal security audit to identify vulnerabilities and validate security controls across the platform
- Developing monitoring and logging capabilities for security event detection and incident response
- Built AI-powered voice agent using n8n workflows to answer cybersecurity questions and provide interactive learning support
- Developed AI automation agents for job search monitoring (8-hour email notifications) and recruiter screening workflows

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

Owner & Operations Manager | JKM LLC | 2021 – 2025

- Investigated and resolved access control, system configuration, and payment security incidents
- Implemented security controls aligned with FISMA Low/Moderate principles and managed user access provisioning
- Developed SOPs for secure system configuration and compliance documentation

Impact: Reduced food waste from 10% to 1% through tech-enabled operational improvements

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

- Supported IAM provisioning, access reviews, and troubleshooting across AWS and Bitbucket
- Performed periodic access reviews aligned with NIST AC controls (AC-2: Account Management, AC-3: Access Enforcement)
- Investigated authentication failures and documented security findings for escalation

Impact: Contributed to successful ServiceNow integration and 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