AKSHAY RAJ

Senior Cybersecurity Engineer – AI Security & SIEM Architecture

DevSecOps | ISO 27001 & GRC (NCA / SAMA)

Dubai, UAE | +971 556033027 | sendingtoakshay@gmail.com | linkedin.com/in/akshayrajkollam

PROFESSIONAL SUMMARY

Senior Cybersecurity Engineer with 4 years of hands-on experience spanning AI-augmented security operations, SIEM architecture, DevSecOps, and GRC. Led the design and automation of a production Wazuh/OpenSearch SIEM platform, deployed an AI/ML-driven Web Application Firewall (OpenAppSec) for adaptive threat prevention, and integrated AI agents (including Hermes) for automated log analysis and CI/CD security. Delivered ISO 27001 certification and managed NCA and SAMA compliance for a financial product used by tier-1 banks including Al Rajhi Bank, D360 Bank, Vision Bank, ez bank (Ajlan), and Bank of Jordan. Identified a critical SQL injection exposing 30,000+ customer records with plaintext passwords, and reduced mean time to detect (MTTD) by 42%.

PROFESSIONAL EXPERIENCE

Senior Security Engineer

Interland Technology Services Pvt. Ltd. (Alfaris Group), Thiruvananthapuram, India | Aug 2022 – Jun 2026

- **Automated SIEM Architecture & SOC Operations:** Led the end-to-end design, deployment, and automation of a production-grade Wazuh/OpenSearch SIEM platform using ClickHouse and Vector for high-volume log ingestion. Integrated TheHive for centralized alerting and incident management. Streamlined SOC workflows using Ansible Semaphore and GLPI, reducing MTTD by 42%.
- **AI-Powered Security Automation & AI Firewall Deployment:** Deployed and configured OpenAppSec, an AI/ML-based Web Application Firewall, delivering automated, self-learning threat detection and blocking of OWASP Top 10 attacks without manual rule tuning. Implemented AI agents (including Hermes) for intelligent log analysis, anomaly detection, and automated security checks within CI/CD pipelines, improving detection accuracy and reducing manual analysis effort.
- **Product Security & Compliance (ISO 27001, NCA, SAMA):** Led end-to-end ISO 27001 certification for the organization and managed NCA (Saudi Arabia) and SAMA compliance requirements for a financial product used by tier-1 banks including Al Rajhi Bank, D360 Bank, Vision Bank, ez bank (Ajlan), and Bank of Jordan. Achieved a 100% audit pass rate with zero critical findings.
- **Vulnerability Management & Application Security:** Conducted penetration testing across multiple web applications targeting OWASP Top 10 vulnerabilities (SQL injection, IDOR, SSRF, broken authentication, account takeover). Integrated Trivy and Bearer into GitLab CI/CD pipelines and tracked remediation of 1,200+ vulnerabilities under a strict 48-hour SLA.
- **DevSecOps & Secure SDLC:** Designed and implemented shift-left security pipelines using SonarQube (SAST), Trivy, and Bearer across Java Spring Boot and Angular applications. Embedded security controls and AI-assisted checks into the development lifecycle.
- **Cloud & Container Security:** Secured 30+ Kubernetes pods using Falco runtime threat detection and enforced container security best practices.
- **Network & Identity Security:** Configured Netbird Zero Trust architecture and worked with Fortinet and Palo Alto firewalls. Implemented Zitadel (OIDC/OAuth 2.0) across 15+ applications, eliminating 95% of credential-based attack surface.
- **Infrastructure Monitoring & IT Asset Management:** Deployed Zabbix and Grafana for unified visibility and Snipe-IT for complete asset inventory and vulnerability mapping.

TECHNICAL SKILLS

- **SIEM & Security Operations:** Wazuh, OpenSearch, TheHive, ClickHouse, Vector, Zabbix, Grafana, Suricata, Falco, SOC Automation
- **AI & Security Automation:** AI Agents, Hermes, AI-Powered WAF / AI Firewall Configuration (OpenAppSec), AI-Driven Log Analysis, Automated Security Checks in CI/CD, Ansible
- **DevSecOps & Application Security:** GitLab CI/CD, SonarQube (SAST), Trivy, Bearer, Secure SDLC, OWASP Top 10, Burp Suite
- **Cloud & Container Security:** Kubernetes Security, Docker, Falco, Container Hardening, CSPM
- **Network & Zero Trust:** Fortinet, Palo Alto, OpenAppSec AI Firewall / WAF, Netbird, Network Segmentation
- **Identity & Access Management:** Zitadel, OIDC, OAuth 2.0, SSO, Privileged Access Management
- **Compliance & Governance:** ISO 27001, NCA (Saudi Arabia), SAMA Framework, Risk Assessment, Audit Management
- **Programming & Scripting:** Python, PowerShell, Bash, Java (Spring Boot), Angular, YAML

EDUCATION

Bachelor of Technology (BTech), Computer Science
Bir Tikendrajit University, Manipur | Graduated 2022

CERTIFICATIONS

- Fortinet Network Security Expert (NSE) 1, 2, and 3
- CompTIA Security+ (In Progress)

SECURITY RESEARCH & BUG BOUNTY

- **Critical SQL Injection, UK Government Beverages Agency:** Discovered a time-based blind SQL injection exposing 30,000+ customer records including plaintext passwords. Responsibly disclosed and coordinated remediation.
- **Full Account Takeover, Noise India:** Identified a critical password reset flaw enabling complete account takeover.