AKSHAY RAJ

Cybersecurity Engineer – GRC, Security Operations & Application Security

ISO 27001 | SAMA & NCA Compliance | SIEM & Incident Response | VAPT | DevSecOps

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

PROFESSIONAL SUMMARY

Cybersecurity engineer with 4 years' broad, hands-on experience across **governance, risk & compliance, security operations, application security and incident response** in a regulated financial services environment. Led an organisation-wide **ISO 27001** certification and owned **SAMA and NCA** compliance for a banking platform used by tier-1 institutions including Al Rajhi Bank, D360 Bank, Vision Bank, ez bank (Ajlan) and Bank of Jordan — achieving a **100% audit pass rate with zero critical findings**. Built and operated a production **Wazuh/OpenSearch SIEM** (42% reduction in mean time to detect), ran the full incident response lifecycle, and drove **1,200+** vulnerabilities to closure through penetration testing and DevSecOps pipelines. Equally comfortable writing a control matrix, tuning a detection rule, or exploiting a vulnerability — and translating any of them into clear risk for business stakeholders.

CORE COMPETENCIES

- **Governance, Risk & Compliance** — ISO 27001 implementation & certification, SAMA Cybersecurity Framework, NCA, risk assessment, control design, policy authoring, audit management
- **Security Operations & SIEM** — monitoring, detection engineering, alert triage, threat hunting, log correlation
- **Incident Response** — full lifecycle detection, containment, eradication, recovery, root cause analysis, reporting
- **Application Security & VAPT** — web, API and network penetration testing, source code review, OWASP Top 10 & API Top 10
- **Network & Infrastructure Security** — firewalls, IDS/IPS, WAF, Zero Trust, server and endpoint hardening
- **Cloud & Container Security** — Docker, Kubernetes, runtime threat detection, container hardening
- **Identity & Access Management** — SSO, OIDC/OAuth 2.0, privileged access management
- **DevSecOps** — CI/CD security gates, SAST/SCA, secure SDLC, developer enablement

PROFESSIONAL EXPERIENCE

Senior Security Engineer

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

- **Governance, Risk & Compliance:** Led end-to-end **ISO 27001** certification — ISMS scope, risk assessment and treatment, Statement of Applicability, control design and evidence — and managed **SAMA** and **NCA** compliance for a financial product. Translated regulatory clauses into measurable IT general controls maintained as a control-to-requirement matrix.
- **Audit Management — 100% Pass Rate:** Managed internal audits, external ISO 27001 certification and recurring client-side regulatory audits by **tier-1 bank customers** (Al Rajhi Bank, D360 Bank, Vision Bank, ez bank (Ajlan), Bank of Jordan). Achieved a **100% pass rate with zero critical findings**.
- **SIEM Architecture & Security Operations:** Designed, deployed and operated a production Wazuh/OpenSearch SIEM with high-volume ingestion (ClickHouse, Vector), Suricata IDS/IPS and Falco runtime detection, with TheHive for case management. Authored and tuned custom detection rules, reducing **mean time to detect by 42%**.
- **Incident Response:** Owned incidents through the full lifecycle — detection, triage, containment, eradication and recovery — as senior escalation point, followed by root cause analysis and preventive control changes. Documented every incident to audit standard.
- **Penetration Testing & Vulnerability Management:** Performed web, API and network penetration testing against OWASP Top 10 (SQL injection, IDOR, SSRF, broken authentication, account takeover) with Burp Suite and Nmap. Tracked **1,200+ vulnerabilities** to verified closure under a strict **48-hour SLA**.
- **DevSecOps & Application Security:** Built shift-left security pipelines in GitLab CI/CD — SonarQube (SAST), Trivy and Bearer as enforced gates across Java Spring Boot and Angular applications — with code-level review and developer coaching on secure practice.
- **Network, Cloud & Identity Security:** Configured Fortinet and Palo Alto firewalls and an AI/ML-based WAF; secured 30+ Kubernetes pods with Falco and container hardening; implemented Zitadel SSO (OIDC/OAuth 2.0) across 15+ applications, eliminating **95%** of the credential-based attack surface; and deployed Netbird Zero Trust segmentation.

- **AI-Driven Security Automation:** Deployed an AI/ML Web Application Firewall (OpenAppSec) and integrated LLM-based AI agents for automated log analysis, anomaly detection and security checks within CI/CD pipelines.
- **Enablement & Stakeholder Communication:** Ran security awareness and information security management training across departments, and briefed engineering and business leadership by translating technical risk into business impact.

TECHNICAL SKILLS

- **Governance & Compliance:** ISO 27001 / 27002, ISO 27005, SAMA Cybersecurity Framework, NCA (Saudi Arabia), NIST CSF (working knowledge), risk assessment, control matrices, policy authoring, audit management
- **SIEM & Security Operations:** Wazuh, OpenSearch, ClickHouse, Vector, TheHive, Suricata, Falco, Zabbix, Grafana, detection engineering, threat hunting
- **Offensive Security & VAPT:** Burp Suite, Nmap, OWASP Top 10 & API Top 10, web/API/network penetration testing, source code review, bug bounty
- **DevSecOps & AppSec:** GitLab CI/CD, SonarQube (SAST), Trivy, Bearer, secure SDLC, shift-left security
- **Network & Infrastructure:** Fortinet, Palo Alto, firewall configuration, IDS/IPS, WAF / reverse proxy, Netbird Zero Trust, network segmentation, server hardening
- **Cloud & Container:** Docker, Kubernetes security, container hardening, Falco runtime detection, CSPM concepts
- **Identity & Access:** Zitadel, OIDC, OAuth 2.0, SSO, privileged access management
- **AI Security:** AI/ML WAF (OpenAppSec), LLM-based agents, AI-driven log analysis and anomaly detection
- **Programming & Scripting:** Python, Bash, PowerShell, Ansible, YAML, SQL, Java (Spring Boot), Angular
- **Operating Systems:** Linux (Ubuntu, RHEL/CentOS), Windows (incl. Server), macOS

SELECTED ACHIEVEMENTS & SECURITY RESEARCH

- Delivered ISO 27001 certification and SAMA/NCA compliance for a financial platform serving five tier-1 GCC banks — zero critical findings across all audits.
- Reduced mean time to detect by **42%** through SIEM architecture and detection engineering.
- Discovered a critical time-based blind SQL injection at a UK government agency exposing **30,000+ customer records including plaintext passwords**; responsibly disclosed and coordinated remediation.
- Identified a password reset flaw enabling full account takeover at Noise India; reported and remediated.

CERTIFICATIONS

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

EDUCATION

Bachelor of Technology (B.Tech), Computer Science
Bir Tikendrajit University, Manipur, India | Graduated 2022