Sarthak KC

Kathmandu, Nepal • sarthakkc2072@gmail.com • +977-9841997717
LinkedIn • GitHub

Professional Summary

SOC Analyst at a managed security service provider, monitoring Class A and B banks and critical-infrastructure clients across FortiSIEM, LogPoint, and LogRhythm. Hands-on with incident triage, SIEM rule creation and tuning, threat hunting, manual log analysis, and client security reporting. Prior banking internship in VAPT, GRC, and phishing simulation. Certified LLM Security Expert currently building an AI Detection and Response (AIDR) prototype, and ranked 1st in Nepal and 32nd globally on Blue Team Labs Online.

Key Achievements

- Ranked **1st in Nepal** and **32nd globally** on Blue Team Labs Online (BTLO), a blue-team investigation and CTF platform
- Discovered and responsibly disclosed **CVE-2025-59827**, a missing authorization vulnerability in open-source software

Technical Skills

- **SIEM Platforms:** FortiSIEM, LogPoint, LogRhythm, Wazuh, Security Onion
- **Security Operations:** Alert Triage, Incident Response, SIEM Rule Creation & Tuning, Threat Hunting, Manual Log Analysis, Security Reporting
- **Log Sources:** Windows Security & Sysmon events, Microsoft 365 / Office 365 audit and sign-in logs, MDaemon mail server logs, FortiGate firewall, F5 WAF, DNS, Active Directory & Kerberos
- **Security Testing:** Vulnerability Assessment & Penetration Testing (VAPT), Digital Forensics, Security Auditing
- **Tools:** Faraday, GoPhish, pfSense, Zabbix, mitmproxy, Microsoft Presidio, Python
- **AI & LLM Security:** Prompt injection, RAG poisoning, AI agent security, OWASP Top 10 for LLM Applications, AI data loss prevention
- **Governance & Cloud:** GRC, Risk Assessment, IT Audit, Compliance Reporting, AWS fundamentals

Professional Experience

SOC Analyst *May 2026 – Present*
CryptoGen Nepal, Kathmandu

- Monitor the full client portfolio of Class A and B banks and critical-infrastructure utilities across FortiSIEM, LogPoint, and LogRhythm, triaging and investigating SIEM incidents end to end
- Create and tune SIEM correlation rules to improve detection coverage and reduce false positives based on each client's environment
- Perform manual log analysis of Windows Security/Sysmon events, F5 WAF, FortiGate firewall, DNS, and Kerberos logs to validate findings and support client escalation
- Prepare client-specific security documentation as per each client's requirements
- Produce daily, weekly, monthly, and quarterly security reports covering observed activity, significance, and recommendations
- Conduct threat hunts during night shifts and publish threat hunt reports, including identifying a domain controller audit policy gap (missing Kerberos event logs)
- Prepare festive-season threat advisory reports addressing heightened risk during major holidays
- Perform initial incident response with client teams, support junior analysts, and maintain shift handover documentation

Security Analyst Intern *August 2025 – November 2025*
Jyoti Bikash Bank Limited, Kathmandu

- Executed comprehensive VAPT on banking website and mobile application, identifying critical vulnerabilities and delivering actionable mitigation strategies
- Architected and deployed Faraday vulnerability management platform on internal servers, enabling real-time vulnerability tracking and 40% faster remediation workflows
- Participated in POC evaluation of LogPoint SIEM, assessing log ingestion, correlation rules, and deployment feasibility for enterprise SOC environment
- Developed enterprise-level GRC reports and risk assessments for IT infrastructure, ensuring regulatory compliance and identifying systemic security gaps
- Led departmental IT security audits including PC hygiene assessments, maintaining 95% compliance with internal security standards
- Designed and executed GoPhish security awareness campaign across multiple departments, reducing phishing click-through rates through user engagement metrics

Projects

AI Detection and Response (AIDR) Framework – Final Year Project *2026 – Ongoing*
Presidential Graduate School (team of 3)

- Building a prototype that detects and prevents sensitive data leakage when employees use external generative AI tools (ChatGPT, Claude, Gemini, Copilot)
- Designed a local TLS-intercepting proxy with mitmproxy to capture prompts from both browser and desktop AI clients
- Using NER-based detection (Microsoft Presidio, spaCy) for sensitive data, extended with a risk-scoring engine, policy enforcement, and a SOC-style monitoring dashboard
- Evaluating detection performance with precision, recall, F1, and false positive rate

College SOC Lab Setup *2024 – 2025*
Presidential Graduate School

- Built a Proxmox-based SOC lab for hands-on student training, with VLAN segmentation and a hardened pfSense perimeter firewall
- Deployed Security Onion (Suricata/Zeek, full-packet capture) for network monitoring and Wazuh SIEM for host log collection
- Integrated Zabbix infrastructure monitoring and log aggregation pipelines for real-time detection and incident response practice

Education

Bachelor of Science in Information Technology (Expected Graduation)
Westcliff University, Kathmandu
Higher Secondary Education, Science Stream *2020 – 2022*
Kathmandu Model Secondary School

Certifications & Professional Development

- **Certified LLM Security Expert (CLLMSE)** – Red Team Leaders *Sep 2026*
  - Completed hands-on coursework in LLM security domains: prompt injection, RAG poisoning, AI agent security, and LLM supply chain risk
- **ISC2 Certified in Cybersecurity (CC)** – Foundational cybersecurity principles and best practices
- **AWS Cloud Quest: Cloud Practitioner** – Cloud security fundamentals and AWS basics
- **AWS Academy Cloud Web Application Builder** – Cloud application security and architecture
- **Windows Forensics Certification** – Digital forensics and incident investigation fundamentals
- **Beyond The Basics: Mastering Advanced Digital Forensics Techniques** – Advanced forensic analysis
- **Bug Bounty/Security Researcher Certification (FlagForge)** – Introduction to vulnerability identification and responsible disclosure