SUBASH LAMA

Information Security Analyst | SOC Analyst | IAM Analyst | GRC Analyst

Open to Remote • +977 9840005771 • lamasubash107@gmail.com • linkedin.com/in/subash-lama-b319a016b • github.com/Subash107

PROFESSIONAL SUMMARY

Results-driven Information Security Analyst with 10+ years of hands-on experience across SOC operations, Identity and Access Management (IAM), GRC, and enterprise IT security. Demonstrated success reducing security incidents by 60%, cutting MTTR by 40%, and maintaining 99.9% infrastructure uptime across multi-site environments of 200+ users. Deep expertise in SIEM administration (Wazuh), intrusion detection (Suricata IDS/IPS), threat hunting, log analysis, alert triage, and incident response aligned to NIST 800-61 and MITRE ATT&CK frameworks. Proven IAM skills: Active Directory, RBAC, MFA, SSO, Privileged Access Management, and user lifecycle management. Hands-on GRC experience including vulnerability management, risk assessment, security policy development, and compliance with CIS Controls and ISO 27001. Certified Ethical Hacker (Cisco, 2026) with active bug bounty research. Currently operating a self-built SOC detection lab and seeking a remote mid-level security role.

CORE COMPETENCIES

SOC & Threat Operations: SOC Operations • Alert Triage • Threat Hunting • Threat Detection • Incident Response • Log Analysis • Security Monitoring • Detection Engineering • MTTD/MTTR Improvement

SIEM & Security Tools: Wazuh SIEM • Suricata IDS/IPS • Sysmon • mitmproxy • Pi-hole • Wireshark • tcpdump • Nessus • Zenmap • Burp Suite

Identity & Access Management (IAM): Active Directory • RBAC • Group Policy (GPO) • MFA • SSO • Privileged Access Management (PAM) • User Provisioning & Lifecycle • Zero Trust • Least Privilege

GRC & Compliance: Risk Assessment • Vulnerability Management • Security Policy Development • Security Audits • NIST CSF • NIST 800-53 • NIST 800-61 • ISO 27001 • CIS Controls • Regulatory Compliance

Networking & Infrastructure: Firewalls • VPN • DNS • DHCP • VLAN • Proxy Servers • Cisco • Network Traffic Analysis • Network Security • Routing & Switching

Automation & DevOps: Python • Bash • PowerShell • GitHub Actions (CI/CD) • Ansible • Docker • AWS • Prometheus • Grafana • Infrastructure as Code (IaC) • DevSecOps

PROFESSIONAL EXPERIENCE

Independent Cybersecurity Researcher

Mar 2025 – Present

Self-directed Security Research Lab • *Remote*

- Built and operate a production-grade SOC detection lab — Wazuh SIEM, Suricata IDS/IPS, Sysmon, Pi-hole, mitmproxy — simulating real enterprise SOC operations including alert triage, threat hunting, and incident response across Hyper-V and WSL2 environments.
- Engineered 20+ custom SIEM correlation rules mapped to MITRE ATT&CK techniques, reducing false positive rate and improving mean time to detect (MTTD) across monitored endpoints.
- Authored incident response runbooks and Wazuh alert investigation SOPs aligned to NIST 800-61 lifecycle — published on LinkedIn as open security workflow documentation.
- Researching security data normalization and sensor correlation (CaSOB ontology) to unify heterogeneous telemetry from multiple sensors into a single detection pipeline.
- Automated infrastructure hardening, deployment, and service health monitoring using Python and Bash; applied Infrastructure as Code (IaC) practices for repeatable lab provisioning.
- Active bug bounty researcher on HackerOne, Intigriti, and Bugcrowd — web application vulnerability assessment, responsible disclosure, and CVE documentation.

IT Officer / System & Network Administrator
Jan 2020 – Feb 2025

Primuson Pvt. Ltd. • *Kathmandu, Nepal*

- Owned end-to-end Identity and Access Management (IAM): Active Directory administration, RBAC configuration, Group Policy (GPO) enforcement, Privileged Access Management, MFA rollout, and quarterly access reviews for 150+ users across 5 offices.
- Reduced security incidents by 60% through a structured vulnerability management program — regular vulnerability assessments, penetration testing across 100+ assets, patch management workflows, and system hardening.
- Implemented SIEM-based security monitoring and alert triage workflow, cutting MTTR by 40% and establishing a repeatable incident response process aligned to organizational risk policy.
- Enforced security policies, access control baselines, and system hardening standards aligned to CIS Controls — supporting GRC reporting and audit readiness.
- Managed multi-site network security infrastructure — firewalls, VPN, DNS, DHCP, proxy servers — achieving 99.9% uptime across all locations.
- Deputed as IT Consultant to Aistra Consultancy Co., Ltd. (Phnom Penh, Cambodia) for one year — delivered IT infrastructure support, security advisory, and IAM services as part of a cross-border business partnership.
- Designed and implemented automated backup, disaster recovery, and business continuity solutions — zero data loss incidents over 3 years.

IT Specialist (Contract)
Mar 2018 – Apr 2019

State Bank of India • *Kathmandu, Nepal*

- Managed IAM for 200+ banking staff — Active Directory user lifecycle, RBAC, privileged access controls, and compliance-driven access reviews ensuring zero unauthorized access incidents.
- Administered firewall, proxy server, and network security infrastructure ensuring 100% compliance with enterprise security policy and banking regulatory requirements.
- Led incident response and root cause analysis (RCA) for security events — documented findings, implemented corrective controls, and reported to senior management.
- Reduced system downtime by 30% through proactive security monitoring, vulnerability scanning, and patch management across hybrid infrastructure.

IT Consultant (Contract)
Jan 2017 – Dec 2017

Unilever • *Nepal*

- Administered Cisco network infrastructure, firewall policy, and Active Directory IAM for a 50+ user enterprise environment — zero critical security incidents during full engagement.
- Conducted network security audits and implemented system hardening aligned to corporate security standards and global IT access control policy.
- Delivered secure hybrid IT operations ensuring compliance with Unilever global IT security standards across the Nepal business unit.

Support Engineer
Mar 2016 – Apr 2019

Green IT Solutions Pvt. Ltd. • *Kathmandu, Nepal*

- Delivered IT security support and ICT infrastructure services for 10+ enterprise clients — maintained 98% SLA compliance across incident management, network administration, and vulnerability remediation.
- Administered storage virtualization, proxy servers, and core network services; performed regular security assessments and patch management.
- Resolved 500+ incidents across hardware, software, and network environments — reduced recurrence by 35% through root cause analysis and preventive security controls.

IT Trainee
Mar 2014 – May 2016

Platinum Hotel & SPA • *Kathmandu, Nepal*

- Provided IT support for hardware, software, and network troubleshooting across a 100+ room hospitality facility — maintained daily security operations and end-user access management.
- Reduced average ticket response time by 25% through structured triage and proactive network monitoring.

KEY PROJECTS

- SOC Detection Lab — Wazuh SIEM + Suricata IDS/IPS + Sysmon + mitmproxy + Pi-hole: Production-grade detection environment with 20+ MITRE ATT&CK-mapped custom rules, TLS traffic inspection, DNS monitoring, and published incident response SOPs.
- Bug Bounty Research — Active vulnerability researcher on HackerOne, Intigriti, and Bugcrowd; identified and responsibly disclosed 15+ vulnerability patterns across web application targets.
- CI/CD Security Pipeline — GitHub Actions-based CI/CD with automated security checks and DevSecOps controls; reduced deployment time by 60%.
- Full-Stack Observability — Prometheus + Grafana monitoring across 10+ services; real-time security alerting and proactive incident detection.

CERTIFICATIONS & TRAINING

- Endpoint Security — Cisco Networking Academy (Jun 2026)
- Ethical Hacker (CEH) — Cisco Networking Academy (Apr 2026)
- Google Ads Video Certification — Skillshop / Google (May 2026, expires May 2027)
- Introduction to Cybersecurity — Cisco Networking Academy (Mar 2026)
- Python for Data Science — IBM (Mar 2026)
- Data Analysis with Python — IBM SkillsBuild (Mar 2026)
- Cybersecurity Fundamentals — IBM SkillsBuild (Mar 2026)
- Diploma in DevOps (CI/CD, AWS, Infrastructure Automation) — Deerwalk Training Center, Nepal (2023)
- CCNA — Cisco Certified Network Associate — Staff College, Jawalakhel, Nepal (2016)

TECHNICAL SKILLS

Security & Monitoring: Wazuh SIEM, Suricata IDS/IPS, Sysmon, mitmproxy, Pi-hole, Wireshark, tcpdump, Nessus, MITRE ATT&CK, Vulnerability Assessment, Penetration Testing, Threat Detection, Incident Response, Log Analysis, Alert Triage, System Hardening

Identity & Access Management: Active Directory, RBAC, Group Policy (GPO), MFA, SSO, Privileged Access Management (PAM), User Provisioning, Access Control, Zero Trust, Least Privilege, Windows Server

GRC & Compliance: Risk Assessment, Vulnerability Management, Security Policy, Security Audits, NIST CSF, NIST 800-53, NIST 800-61, ISO 27001, CIS Controls, Regulatory Compliance, Business Continuity, Disaster Recovery

Networking: Firewalls, VPN, DNS, DHCP, VLAN, Proxy Servers, Cisco, Routing & Switching, Network Traffic Analysis, Network Security

Systems & Cloud: Linux (Ubuntu, Red Hat, Debian), Windows Server, Office 365, AWS, Cloud Security, MySQL, VMware vSphere/ESXi, Hyper-V, WSL2, Docker

Automation & DevOps: Python, Bash, PowerShell, GitHub Actions (CI/CD), Ansible, Infrastructure as Code (IaC), Prometheus, Grafana, DevSecOps

EDUCATION

Bachelor of Business Studies — Nepal Mega College *2022*

High School (Computer Science) — Kasthamandap College, Kalanki *2014*

LANGUAGES

Nepali (native) • English (professional working proficiency) • French (elementary, actively studying)