Saksham Sharma

Cybersecurity Analyst | SOC (Blue Team)

sharma@saksham.info.np | contactsaksham52@gmail.com | +977 9764777592 | Lalitpur, Nepal
LinkedIn: sakshamsharma52 | GitHub: unexplainablefish52

Summary

IT undergraduate (TU IOST) focused on **Security Operations (SOC)**, network security, and defensive cybersecurity. Developed practical skills through **home lab** implementation, scenario-based security training, and certifications from reputed organizations and platforms including **Google, ISC2, CompTIA-aligned training, Oracle, and Microsoft**. Experience includes **traffic analysis**, **firewall rule configuration**, **SIEM-based log review**, and **security event investigation fundamentals**. Motivated to contribute to **alert triage**, **threat detection**, incident documentation, and risk-aware security operations in an entry-level SOC or cybersecurity role.

Skills

Operating Systems	Linux, Kali Linux, Windows
Networking	TCP/IP, DNS, HTTP/S, routing concepts, packet capture, traffic analysis
SOC / Blue Team	Alert triage, log analysis, SIEM, XDR and IR Foundations, threat detection
Security Tools	Wireshark, tcpdump, Splunk SPL, pfSense, Nmap, Burp Suite
Documentation	Incident notes, investigation summaries, technical reporting

Hands-on Practice & Home Lab

- Deployed **Wazuh SIEM/XDR** with Windows/Linux agents; investigated endpoint alerts, vulnerable packages, CVE findings, logs, and security posture weaknesses with remediation guidance.
- Captured and analyzed network traffic using **Wireshark** and **tcpdump**, applying protocol and host-based filters across DNS, TCP, HTTP/S, ARP, ICMP, and suspicious connection patterns.
- Configured **pfSense** firewall policies using segmented lab networks, rule-order logic, default-deny design, traffic logging, and controlled access between attacker, victim, and monitoring systems.
- Developed an **incident response playbook** and SOC reporting workflow covering executive summaries, analyst findings and **GRC-style** business impact analysis.
- Used **Nmap** in controlled lab environments for asset discovery, service enumeration, OS fingerprinting, full-port scanning, and exposed-service validation.
- Practiced SOC-style investigation workflows using **Splunk SPL** and **LetsDefend**, documenting indicators, alert context, anomalies, and recommended next-step checks.

Certifications

- **ISC2 Certified in Cybersecurity (CC)** — ISC2 — 2026
- **Google Cybersecurity Professional Certificate** — 2026
- **Google Network Security Specialization** — Coursera — 2025
- **Security+ Training Certificate** — Coursera — 2025

Education

Bachelor in Information Technology (BIT), TU IOST Nov 2024 – Present
Patan Multiple Campus, Lalitpur, Nepal

High School (Science Stream), GPA: 3.43 Aug 2022 – Jun 2024
Madhyabindu Multiple Campus, Nawalpur, Nepal