Sarvesh Khanal

Entry-Level Cybersecurity Analyst

Kathmandu, Nepal | khanal.sarvesh@gmail.com | linkedin.com/in/sarvesh-khanal | github.com/sarvesh-dotcom

Professional Summary

Cybersecurity professional in training with hands-on lab experience in security monitoring, log analysis, and endpoint threat detection using SIEM tooling across Linux and Windows environments. Background in software quality assurance and full-stack development (React.js, Node.js) provides a strong foundation in systems architecture, testing methodology, and analytical troubleshooting. BSc in Computer Science and Information Technology. Seeking an entry-level Cybersecurity Analyst or SOC Analyst role to apply security monitoring, log analysis, and incident-response fundamentals in a professional environment.

Core Skills

Security: SIEM (Wazuh) • File Integrity Monitoring • Threat Hunting • Log Analysis • Vulnerability Assessment • Incident Response Fundamentals • IAM Fundamentals

Systems & Networks: TCP/IP • DNS • HTTP/S • Linux (Ubuntu/Kali) • Windows • Wireshark

Tools & Scripting: Wazuh • Nmap • Burp Suite • Postman • Selenium • Git • Python • Bash • SQL

Hands-On Cybersecurity Projects

SIEM Home Lab – File Integrity Monitoring with Wazuh 2026

- Deployed a Wazuh Manager and Dashboard on Ubuntu 24.04 Server and registered a Windows 10 Wazuh Agent over TCP 1514, building a two-tier lab architecture for centralized endpoint monitoring
- Configured real-time File Integrity Monitoring (FIM) in `ossec.conf` to watch a custom directory on the Windows endpoint for file creation and deletion events
- Validated detection coverage by creating and deleting test files in the monitored directory and confirming corresponding alerts were generated and visualized in the Wazuh Dashboard
- Troubleshot agent-manager connectivity and version compatibility issues during setup, and documented the architecture, configuration, and results for public reference

Threat Hunting with Wazuh SIEM and Sysmon 2026

- Deployed a Wazuh Manager, Indexer, and Dashboard on Ubuntu Server and installed a Wazuh Agent on Windows 11, building a two-tier lab architecture for centralized endpoint monitoring
- Installed and configured Sysmon using the SwiftOnSecurity configuration to capture detailed Windows telemetry, forwarding process creation, PowerShell execution, and user-enumeration events to Wazuh for analysis
- Simulated common Windows attack-adjacent activities (process creation, PowerShell and Command Prompt execution, `net user` enumeration) and analyzed resulting alerts in the Wazuh Dashboard to validate detection coverage
- Documented the lab architecture, detection scenarios, and findings in a written report, and sanitized configuration files (`ossec.conf`, `sysmonconfig.xml`) for public reference

Education & Certifications

Bachelor of Science in Computer Science and Information Technology (BSc CSIT) 2026
Institute of Science and Technology (IOST), Tribhuvan University *Kathmandu, Nepal*

Certifications: API Testing Path (v12) • Python and Django • Learn Node.js • Namaste React
Currently pursuing a Cybersecurity Fundamentals course covering security monitoring, threat analysis, and SIEM operations

Experience

Web Developer Nov 2025 – Feb 2026
Brandworth Pvt Ltd *Kathmandu, Nepal*

- Gained hands-on exposure to full-stack system architecture by building and integrating RESTful APIs with Node.js and SQL, developing a practical understanding of how applications, data, and infrastructure connect
- Practiced systematic, detail-driven testing methodology by using Selenium and Postman for functional and API testing, building transferable skills for security analysis and vulnerability assessment
- Resolved bugs across front-end and back-end systems by debugging React.js and Node.js code, reinforcing an analytical, root-cause mindset applicable to security investigation and log analysis

Additional

Open to: Entry-level Cybersecurity Analyst, SOC Analyst, and Security Operations roles
Interests: Security Operations • Threat Detection • Vulnerability Management • Network Security