Binod Rawat

Kathmandu, Nepal
9849384491 || binod.codes@gmail.com || binod-rawat

Professional Summary

SOC Analyst with 6 months of professional experience in Security Operations Center (SOC) environments, specializing in security monitoring, alert triage, threat hunting, incident response, and log analysis. Experienced in Falcon NG-SIEM, detection engineering, CQL query development, dashboard customization, correlation rule creation, and centralized log management across Windows, Ubuntu, Linux, and pfSense environments. Skilled in investigating phishing, malware, authentication anomalies, and network-based threats while reducing false positives through detection tuning. Strong understanding of MITRE ATT&CK, threat intelligence, IOC analysis, and defensive security operations. Passionate about strengthening enterprise security through proactive monitoring and continuous improvement.

Education

Amrit Science Campus — Kathmandu, Nepal
Bachelor in Information Technology (BIT) — *Graduated: 2025*

Professional Experience

SOC Analyst — Jan 2026 – Present
Raechal Enterprises Pvt. Ltd. — *Kathmandu, Nepal*

- Performed continuous security monitoring, alert triage, incident investigation, and log analysis using Falcon NG-SIEM.
- Conducted proactive threat hunting to identify Indicators of Compromise (IOCs), suspicious activities, and anomalous behavior across enterprise environments.
- Developed and optimized CQL queries to improve threat detection, investigation efficiency, and SOC visibility.
- Configured centralized log ingestion from Windows, Ubuntu, Linux servers, and pfSense firewall devices into Falcon NG-SIEM.
- Designed SIEM dashboards for improved visibility, security monitoring, and operational efficiency.
- Developed correlation rules and detection logic to improve alert accuracy and significantly reduce false positives.
- Investigated phishing attacks, malware detections, brute-force attempts, privilege escalation events, and authentication anomalies following incident response procedures.
- Prepared technical threat reports documenting investigations, attack timelines, root cause analysis, and mitigation recommendations.
- Created SOC investigation workflows to standardize incident analysis and improve analyst response time.
- Worked closely with security teams to validate incidents, enhance detection capabilities, and continuously improve SOC operations.

Technical Skills

SIEM & Security Operations: Falcon NG-SIEM, Security Monitoring, Alert Triage, Incident Investigation, Detection Engineering, Security Event Correlation

Threat Detection: Threat Hunting, IOC Analysis, Threat Intelligence, MITRE ATT&CK Framework, Malware Analysis, Phishing Investigation

Networking: TCP/IP, OSI Model, Routing, Switching, DHCP, DNS, VPN, Subnetting

Operating Systems: Windows, Ubuntu Linux

Query Languages: CrowdStrike Query Language (CQL)

Security Technologies: Firewall, IDS/IPS, EDR/XDR, MFA, PAM, RBAC, AAA

Protocols: HTTP, HTTPS, SSH, FTP/SFTP, SMTP, DNS, ICMP, ARP

Standards: ISO/IEC 27001

Tools & Technologies

- **SIEM Platforms:** Falcon NG-SIEM, Wazuh
- **Detection Engineering:** CrowdStrike Query Language (CQL), Correlation Rules, Dashboard Customization, Workflow Automation, Log Ingestion
- **Threat Intelligence:** VirusTotal, AlienVault OTX, MISP, AbuseIPDB, URLhaus
- **Network Analysis:** Wireshark, TShark, tcpdump, pfSense
- **Security Assessment:** Nessus Essentials, Nmap

Certifications

Falcon NG-SIEM Specialist	CrowdStrike University
Falcon Administrator	CrowdStrike University
Threat Hunter	CrowdStrike University
Incident Responder	CrowdStrike University
Exposure Management Specialist	CrowdStrike University
AI Security	CrowdStrike University
Certified Blue Team Practitioner (CBTP)	The SecOps Group
Certified Network Security Practitioner (CNSP)	The SecOps Group
Google Cybersecurity Professional Certificate	Coursera
Security Operations Center (SOC)	Coursera

Training

Broadway Infosys — Kathmandu, Nepal
Certified Ethical Hacking (CEH Training) — *2.5 Months*