Bishal Bhandari

Security Researcher | OSINT & Threat Intelligence
Kathmandu, Nepal
bishalbhandari390@gmail.com | +977 9864958063
LinkedIn: linkedin.com/in/bishalbhandari-infosec

Professional Summary

Security and intelligence-focused professional with experience in SOC operations, open-source intelligence (OSINT) research, and digital investigations. Skilled in threat attribution, person-of-interest investigations in a digital context, and intelligence-style reporting using BLUF methodology. Experienced in SIEM monitoring, vulnerability assessment, and automation-driven investigation workflows.

Core Competencies

- Open-Source Intelligence (OSINT) Methodologies
- Person-of-Interest Investigations (Digital Context)
- Threat Attribution & Actor Profiling
- Social Media & Online Presence Reconnaissance
- Deep & Dark Web Threat Awareness
- Intelligence Reporting (BLUF Model)
- Incident Investigation & Documentation
- Fast-Paced Analytical Decision Support

Technical Skills

- **SIEM & Monitoring:** LogPoint (Proficient), Splunk (Familiar), Alert Triage
- **VAPT Tools:** Nmap, Burp Suite, OWASP ZAP, Nikto
- **Threat Analysis:** MITRE ATT&CK, Chainalysis (Blockchain), OSINT methodologies, attribution analysis, threat actor profiling
- **Programming:** Python (Security Scripting), Java, JavaScript, TypeScript
- **Systems:** Windows/Linux, OSQuery, Windows Event Logs
- **Incident Response:** Security Incident Documentation, Threat Hunting
- **Forensics:** Network Forensics, Digital Forensics, person-of-interest research, timeline reconstruction
- **Compliance:** PCI-DSS Fundamentals
- **Endpoint Security:** OSQuery, Windows Event Log Analysis
- **Process Automation:** N8N, Python (Automation Scripting)
- **OSINT & Investigations:** Whois, DNS analysis, Ping, Traceroute, social media reconnaissance, deep & dark web monitoring

Experience

Monal Tech PVT. LTD., Kathmandu

Security Researcher | Jun 2023 - Present 2+ years

- Conduct threat and intelligence investigations by continuously monitoring SIEM alerts for suspicious entities, actions, and evidence of compromise.
- Reduced alert fatigue by 15% through LogPoint filter optimization.
- Conduct vulnerability scans for client networks with Nmap/Burp Suite.
- Cut vulnerability scan time by 10% with Nmap scripting.
- Conduct person-of-interest investigations using blockchain transaction analysis to identify wallets, behavioral patterns, and potential unlawful conduct.
- Built n8n automation workflows to parse security alerts from email, enrich with threat intelligence, and deliver actionable notifications to messaging platforms.
- Conducted open-source intelligence (OSINT) research on public data sources to support incident investigations and contextual threat analysis.
- Prepare technical reports for stakeholders.

Project

MakeMyScan Security Tool | Python, Django | 2024 - Present

- Building Python-based network vulnerability scanner with automated scanning utilities.
- Developing REST APIs for scan management and CVE lookup integration.
- Creating OWASP-aligned web application scanner prototype.

Certifications

- PCI Compliance (Qualys) | 2024
- OPSWAT File Security Associate (OFSA) | 2024
- Ethical Hacking Essentials | 2024

Education

Aadim National College

Affiliated by Tribhuvan University (TU)

Bachelor's in Computer Applications (BCA)

December 2019 – January 2025

- Duration Extended due to COVID-19 disruption.
- Built web/mobile applications with Python and Java, developing transferable skills in:
    - Secure coding practices.
    - Problem-solving for complex systems.
    - API development fundamentals.
- Enhanced collaboration skills through team-based academic projects.