Kripesh Shrestha

Information Security Analyst · Kathmandu, Nepal

kripesh.shrestha10.ks@gmail.com github.com/kripesh01
linkedin.com/in/kripesh-shrestha-196655165 otx.alienvault.com/user/kripesh01/pulses
kripeshshrestha.com.np

SUMMARY

Information security analyst at Nepal Clearing House Limited (NCHL), operator of the ConnectIPS national payment platform. Blue-team practitioner with an offensive foundation (CEH, VAPT program ownership) and a GRC lens (ISO 27001, ISO 42001, PCI DSS). I build in-house threat intelligence, SIEM and fraud-hunting tooling. 5+ years across networking, banking security and payment-infrastructure defence.

EXPERIENCE

Information Security Analyst, Nepal Clearing House Limited (NCHL) Apr 2026 – Present
Kathmandu

- Lead threat intelligence and phishing incident response for ConnectIPS, including live response to organized campaigns that impersonate it.
- Designed and built the in-house phishing intelligence platform: look-alike domains are caught at registration, scored and turned into takedown requests with tamper-evident evidence.
- Build SIEM/SOAR, DLP and MFA tooling in-house, alerting through Wazuh.

Assistant Information Security Officer, Siddhartha Bank Limited Oct 2022 – Apr 2026
Kathmandu

- Owned the VAPT program for internet banking, mobile, payment and AI-enabled applications, with internal teams and external vendors.
- Deployed centralized MFA across the bank's Windows estate.
- Handled incident response, policies and internal audits against ISO 27001, NRB and PCI DSS requirements, monitoring with LogRhythm and Wazuh.

Network/System Administrator, Civil Aviation Authority of Nepal May 2021 – Dec 2022
Tribhuvan International Airport

- Ran Cisco Nexus, Catalyst and Firepower infrastructure in the airport data centre.
- Set up server and network monitoring with Zabbix, Observium and Cacti.
- Responsible for the data centre's physical and logical security.

Lecturer (Networking), Texas College of Management & IT May 2021 – Present
Kathmandu

- Teach networking to Bachelor's students, from theory to hands-on labs.
- Mentor students on academic and career choices, and assess them through projects and exams.

Enterprise Support Officer, Websurfer Nepal Nov 2020 – Jul 2021
Kathmandu

- Configured BDCOM, Huawei and Cisco NCS, ASR and Nexus devices for enterprise customers.
- Configured MikroTik wireless and monitored the network with OpenNMS, Cacti, Zabbix and Nagios.

Technical Support Specialist, Vianet Communications Jan 2019 – Nov 2021
Kathmandu Valley

- Solved customers' technical issues and scheduled field visits.
- Trained and supported newly joined staff.

SKILLS

Security operations & detection	Wazuh, OpenSearch, SIEM/SOAR, Custom detection rules, UEBA baselining, Threat-hunting playbooks
Threat intelligence & IR	Phishing incident response & takedowns, CT log monitoring, Domain-permutation analysis (dnstwist), OSINT, Dark-web & leak-site monitoring, IOC sharing (OTX, CERT coordination)
Offensive security / VAPT	Web, mobile & API testing (Burp Suite), Network testing, Wireshark packet analysis, Metasploit, Wireless attacks (lab)
Data protection & identity	Endpoint DLP (Git pre-push controls, card-data discovery), privacyIDEA MFA, AD/LDAP, Windows Credential Provider, Linux PAM, GPO / Intune deployment
Governance, risk & compliance	ISO/IEC 27001:2022, ISO/IEC 42001, PCI DSS, Policies & audits, BCP/DR documentation
Engineering & infrastructure	Python, PowerShell, Bash, SQL, Flask, Docker, MariaDB, SQLite, MinIO, Local LLMs (Ollama), Cisco Nexus, Catalyst, Firepower, Huawei, MikroTik, Zabbix, Cacti, Observium
Languages	English, Nepali, Hindi

CERTIFICATIONS

Certified Ethical Hacker · EC-Council

Computer Hacking Forensic Investigator · EC-Council

ISO/IEC 27001:2022 Lead Auditor · Mastermind

ISO/IEC 42001 Lead Auditor

Certified Threat Intelligence & Governance Analyst · Red Team Leaders

Cisco Certified Network Associate · Cisco

EDUCATION

Master of Computer Science (MCS), Texas College of Management & IT (Nov 2021 – Apr 2024)

BCS (Hons), Network Technology & Cybersecurity, Texas College of Management & IT (Sep 2017 – Sep 2021)

RESEARCH

Cyber Security Framework for Mitigating Cyber Threats in Banking Payment System in Nepal. Master of Computer Science, Texas College of Management & IT (Lincoln University). Proposes a cyber security framework for tackling cyber threats in Nepal's banking payment systems.

BGP prefix hijack simulation. Research project that simulated an IP prefix hijack on a GNS3 network, submitted in the fifth semester of my BCS at Texas College of Management & IT.

AWARDS AND TRAINING

Cisco APJC NetAcad Riders: 2nd place (2022). Second place in Cisco Networking Academy's regional networking-skills competition.

Team Leader, Teach For Nepal walkathon (2018). Led a team in a 700-person charity walk for public-school students who walk for hours to reach school.

Two-week cyber security training for government IT officers, One Cover Pvt. Ltd., at the Training Institute for Technical Instruction (TITI). Ran the live demos: reading clear-text Telnet and HTTP traffic in Wireshark; generating a payload with msfvenom to show how Android phones and Windows PCs get compromised; monitoring systems with Zabbix, Observium and Cacti to catch failures early.