



Nilaa MAHARJAN

Saarbrückerstrasse, Saarbrücken, Deutschland

+4915216742773 | nilaamhr@gmail.com

[github](#)

[linkedin](#)

[website](#)

PROFILE

Cybersecurity professional with 5+ years of experience in security analytics, incident response, and malware detection. Holds multiple certifications, including CEH and Blue Team Level 1, and a Master's in Cybersecurity. Seeking roles as Cybersecurity Analyst, Security Researcher, SOC, or Incident Responder.

PROFESSIONAL EXPERIENCE

WORKING STUDENT AS SECURITY ANALYTICS ENGINEER (PART TIME)

07/2023-02/2025

SCHWARZ IT KG, HEILBRONN, GERMANY

- Optimized threat detection capabilities and developed use cases with organizational threat models.
- Developed in-house macro detection tool with SIEM integration.
- Created infrastructure automation with Terraform, Ansible and Azure Devops for on-demand malware analysis lab.

ASSOCIATE SECURITY ANALYTICS ENGINEER (FULL TIME)

02/2022-03/2023

LOGPOINT PVT. LTD, LALITPUR, NEPAL

- Analyzed TTPs and created detailed reports and detection rules for APTs, malware and CVEs.
- Created log normalization packages for various vendors.
- Led Emerging Threat Protection Services and published blogs, papers and reports. Available from: [🔗](#)
- Built ready-to-ship customized security playbooks using LogPoint SOAR based on threat intel.

APPLICATION SECURITY ENGINEER (FULL TIME)

08/2020-11/2021

DIGITAL NETWORK SOLUTIONS, KATHMANDU, NEPAL

- Planned and implemented network design and architecture for mid to large and governmental organizations.
- Provided customer support for F5 BIG-IP, GSLB, Cloudflare, Nutanix, VMWare.

INFORMATION SECURITY ANALYST (PROJECT)

01/2020-02/2020

NCELL PVT. LTD

- Tested internal and external web portals for bugs, issues, and vulnerabilities and reported them.
- Localized, set up, and ran Minimum Baseline Security Standard(MBSS) checks as provided by the acquired company.

WEB SECURITY RESEARCHER (INTERN)

08/2019-11/2019

EMINENCE WAYS, KATHMANDU, NEPAL

- Created reports, Proof of Concepts (PoCs), and attack scenarios with NIST and OWASP-recommended methodologies

EDUCATION

MSc. CYBERSECURITY

2023-ongoing

UNIVERSITÄT DES SAARLANDES, SAARBRÜCKEN, GERMANY

- **Thesis:** SOK: Phishing for Standards: A Systematic Review of Social Engineering Measurement Frameworks

BSc. NETWORKING AND IT SECURITY

2017-2020

LONDON METROPOLITAN UNIVERSITY, LONDON, UNITED KINGDOM

- **Thesis:** [Web based Anomaly Detection System using Machine Learning](#)

CERTIFICATIONS

ISO/IEC 27001:2022 LEAD AUDITOR

04/2025

BLUE TEAM LEVEL 1

01/2023

CERTIFIED NETWORK SECURITY PRACTITIONER

03/2023

BLUE TEAM LEVEL 1

01/2023

CERTIFIED ETHICAL HACKER

12/2021

VIEW ALL: [🔗](#)

SKILLS

PROGRAMMING LANGUAGES	Experienced: Python Bash Familiar: HCL YAML PowerShell BASH
CYBERSECURITY & SECURITY ANALYTICS	SOC Operations SIEM (Splunk, LogPoint, ELK) Threat Hunting Incident Response
FRAMEWORKS & TOOLS	MITRE ATT&CK Nessus Wireshark Burp Suite OSINT Tools
OFFENSIVE SECURITY	Penetration Testing Bug Bounty Web Application Security
DEFENSIVE SECURITY	Digital Forensics Endpoint Security Firewalls (F5, Fortinet) Cloud Security
NETWORKING & ADMIN	CCNA Customer Success JIRA Azure Devops
LANGUAGES	Native: Nepal Bhasa Nepali Fluent: English Hindi Beginner: German (A2)

EXTRA

- Lichess: Bullet Elo: 1900, Blitz 1700
- Online store selling artworks: [Decorathi](#)
- Chairman of the local volunteering branch: Rural First Responders - World Vision International