Nilaa MAHARJAN

Sulzbachstr., Saarbrücken, 66125
+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

- 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

- 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

- 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 Researched (Intern)
08/2019-11/2019

EMINENCE WAYS

- Created reports, Proof of Concepts (PoCs) and attack scenarios.
- Tested web applications based on OWASP top 10, enumerated findings, calculated criticality scored based on NIST and reported them to clients.

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

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

- Chess: Bullet Elo: 1900, Blitz 1700
- Online store selling artworks: Decorathi
- Chairman of the local volunteering branch: Rural First Responders - World Vision International