NILAA MAHARJAN [He/Him]

Sulzbachstr., Saarbrücken, • Saarland, Germany • +4915215806312 • nilaamhr@gmail.com

Origin: Kathmandu, Nepal

SUMMARY

Results-oriented cyber security professional with over 4 years of industry experience in various domains of cyber security. Quick learner with an interest to work in close-information-sharing group.

Proven track record in wide ranging global industries, private and governmental organizations, delivering value in Offensive, Defensive, Forensics and Consultancy.

EDUCATION

Master in Cybersecurity, Computer Science
Saarland University, Saarland, Germany (April 2023-2025, TBD)
Bachelor in Networking and IT Security, Computer Science (Hons)
London Metropolitan University, London, UK (August 2017-2021, 81%)

LANGUAGES

Nepal Bhasa (Mother Tongue), Nepali (National Language), English (C1, Working Proficiency), Hindi (Working Proficiency), German (A1, Basic Conversational)

PROFESSIONAL EXPERIENCE

SCHWARZ IT, Heilbronn, Germany **07/2023 – Ongoing**
Security Analytics Engineer, Research and Development (Studentwerker)

Schwarz IT manages the entire digital infrastructure and all software solutions for all users in their retail divisions Lidl and Kaufland, Schwarz Production and the environmental service provider PreZero. It has broad expertise in all areas of IT – from classic software development and IT consulting to AI applications and IT security. This makes Schwarz one of the largest German players in the IT industry and also offers a cloud for the external market with STACKIT.

Major Tasks:

Tuning existing Use Cases and Runbooks and creating new where necessary based on the needs of the company and threat model.
Researching and developing in-house malicious macro detection tool. Incident
Detection and Response.

LOGPOINT PVT. LTD, Lalitpur, Nepal **02/2022 – 03/2023**
Associate Security Analytics Engineer

Logpoint is a privately held cybersecurity company headquartered in Copenhagen, Capital Region. It provides a converged cybersecurity platform that empowers organizations to thrive in a world of evolving threats.

Major Tasks:

Demonstrated research capabilities by analyzing, and creating content based on a wide variety of commodity and APT-based malware and techniques.
Led Emerging Threat Protection Services and published blogs, papers and reports available from: https://www.logpoint.com/en/?s=nilaa+maharjan
Interpret Threat intelligence's IOCs and use them efficiently for creating and distributing alert queries, dashboards and other data visualizations.
Translated research and analytical findings into security use
Built defensive, highly customized security playbooks using the LogPoint SOAR platform. Create technical documentation, end of the year reports from Security Team and research papers around the content deployed to the SIEM.

DIGITAL NETWORK SOLUTIONS (DNS), Kathmandu, Nepal **08/2020 – 11/2021**
Application Security Engineer

Digital Network Solution Pvt. Ltd is an ISO 9001:2015 and ISO 27001 Complaint Certified IT service Provider Company based in Kathmandu, Nepal. They provide Digitization Services and Technology Solutions including Networking, Cybersecurity, Server Infrastructure, IT Consulting, Managed Service, Professional Services and Cloud-based Solutions. The solutions are suited to various industries like Banking, Financial Services and Insurance, Enterprises, Healthcare, Education & the Public/Government sector.

Major Tasks

Deployed and provided support for BIG-IP F5 Web Application Firewall at various reputed institutions.
Planned and implemented Network Design and Architecture for Network and Application Security (Firewall, DNS, DHCP, VPN, NAT Routing, Load Balancing, TCP/IP, Packet Capture and Analysis).
Created reports drafts, Proof of Concepts, deployment scenarios, Support reports and Root Cause Analysis Reports.
Deployed and provided support for Global Server Load Balancing (GSLB) services.
Provided customer support on HCI's, Cloudflare DNS and WAF for quick deployments and product support.

NCELL PVT. LTD, Kathmandu, Nepal **01/2020 – 02/2020**
Information Security Analyst

Ncell Axiata Limited (Previously Ncell Private Limited) is the first private mobile service provider operating in Nepal. The company is committed to building the best-in-class mobile network experience, connecting some of the remotest areas of Nepal with digital communication offerings.

Major Tasks

Tested the company web portal for bugs, issues, and vulnerabilities and reported them immediately.
Took a hands-on approach with network security operations.
Conducted System/Network scanning and auditing for monthly threat and security vulnerability assessment.
Ran, administered, and reported on monthly Nessus scans, compliance checks, and general reports.
Created reports drafts, Proof of Concepts, attack scenarios for the tests, and immediate disclosures.
Localized, set up, and ran Minimum Baseline Security Standard checks provided by the parent company.
Created awareness content as training materials for employees to be used within the entire corporation.
Identified and presented the performance of proactive all-source research to identify and characterize new threats, vulnerabilities, and risks to the customer security context.

EMINENCE WAYS, Kathmandu, Nepal **01/2020 – 02/2020**
Web Security Researcher

Eminence Ways " A Dedicated Cyber Security Company", circles around a group of Cyber security Professions,, who use their expertise in taking security of Information systems to the utmost level.

Major Tasks
Familiarized with ethical hacking methodologies and adhered to accepted laws and technologies.
Took a hands-on approach with web security operations.
Was responsible for understanding and enumerating attacks, calculating the criticality score based on NIST, and the controls, problems, and infrastructure specific to the organization.
Was responsible for scanning and testing web applications set as scope for vulnerabilities, bugs, and issues.
Created reports drafts, Proof of Concepts, and attack scenarios in formal reports to be sent to clients.

PUBLICATIONS

Web Based Anomaly Detection System Using Machine Learning
A project created in python that demonstrates using Machine Learning (Decision Tree and Logistic Regression) on unlabeled HTTP logs to detect potential threats. The report consists of a survey to determine the need, proper literature reviews, an in-depth comparative analysis, and detailed test cases. Loading a python script hosts a local server allowing the user to upload the unlabeled HTTP log, which is labelled and detected. The data is then displayed on a GUI hosted locally.

Emerging Threat Protection - Logpoint
An initiative to produce in-house research to detect, analyze and respond to cyber threats including but not limited to ransomware, CVEs, APT, and campaigns.

Demonstration of Mass JavaScript Injection for Cryptojacking using MITM
Demonstration of simplicity and dangers crypto-jacking attack performed on a public network, a detailed overview and its defense techniques.

Overview of the need of Security Policy in an organization.
A report based on the NIST framework to discuss an overview of security policy and its need in an organization and how to choose the right policy for you.
In-depth look at SQLi as an attack medium: An attacker and a defenders' perspective A detailed overview of SQLi as an attack vector; how to execute the attack and how to defend.

CERTIFICATIONS

Certified Appsec Practitioner (CAP)
Blue Team Level 1
Certified Ethical Hacker (CEH)
Certified in Cybersecurity (ISC2)
Foundations of Operationalizing MITRE ATT&CK [05/2022]
Lean Foundations Professional Certification (Lfpc™)
Cloudflare Accredited Configuration Engineer
Cloudflare Accredited Service Architect
ICSI | CNSS Certified Network Specialist
ISO/IEC 27001 Information Security Associate
Aviatrix Certified Engineer - Multi Cloud Network Associate
Cloudflare Accredited Sales Professional
Multi-Cloud Networking Associate
Cyber Security Foundation - CSFPC™
NSE 1 Network Security Associate (Fortinet)
NSE 2 Network Security Associate

VOLUNTEERING

Rural First Responders - World Vision International [Kirtipur, Kathmandu, 2018 – Current]
Vulnerability and Capacity Assessment - CWIN/World Vision [Kirtipur, Kathmandu, 2018 – Current]
Nepal Scouts [Lalitpur, 2023 – Current]