

# Mahin Arafat

(Green Card Holder/Permanent Resident)

[mahinarafatmeem@gmail.com](mailto:mahinarafatmeem@gmail.com) | 516-618-7416 | Queens, NY (Open to Relocate)

[LinkedIn](#) | [GitHub](#) | [Portfolio Site](#)

Experienced cybersecurity professional with a global background, having worked and studied internationally. Holds advanced degrees and has a proven track record in enhancing security protocols and reducing incidents through innovative technologies. Skilled in various IT fields, including threat detection, digital forensics, and cloud security. Outside of work, I enjoy playing guitar, taking photos, and writing blogs.

## Certifications and Publications

CompTia Security+, CompTia, 2023 ([badge link](#))

AWS Certified Cloud Practitioner, Amazon Web Services Training and Certification ([badge link](#))

Qualys Vulnerability Management Foundation, Qualys Community (In Progress)

Development of a ML-Based Safety-Critical Fire Detection System, Springer Nature Singapore ([link](#))

## Education

Cloud Computing Advanced Training Program

Masters of Electrical and Computer Engineering

Bachelor of Computer Science (Software Engineering)

Npower, New York, USA

Ontario Tech University, Oshawa, Canada

University of Malaya, Kuala Lumpur, Malaysia

## Experience

### Cybersecurity Engineer

January 2024 – Present

Cyberpro Solutions | Remote

- Constructing a virtual lab environment to simulate and identify vulnerabilities, enhancing practical skills in threat detection and mitigation.
- Conducting **Digital Forensics and Incident Response**, performing **Vulnerability Assessments**, and utilizing **Searchsploit** for security assessments.
- Implementing secure and scalable cloud infrastructure in **AWS**, utilizing **EC2 instances**, **S3 for storage**, and **IAM** for secure access management and set up monitoring with **CloudWatch** to track system health, ensuring high availability and performance in production environments.
- Using **NMap** and commands to scan networks on the system and building the project – [sample video](#).
- Implement secure cloud configurations using Azure Private Link, Network Security Groups, Microsoft Defender for Cloud, and Azure Regulatory Compliance for **NIST 800-53**, **PCI DSS**, and **HIPAA/HITRUST**, resulting in a **97% reduction** in security incidents over the same time interval.

### Cyber Threat Investigator

September 2022 – December 2023

Strativ BD Limited | Dhaka, Bangladesh

- Enforced stringent **cybersecurity protocols**, markedly diminishing the frequency of security incidents and associated risks.
- Efficiently identified, scrutinized, and neutralized security breaches to curtail potential harm and safeguard company systems & data, utilizing open-source resources such as **VirusTotal**, **Urlscan**, among others.
- Led the charge in rectifying security breaches, performing thorough **risk and threat evaluations**.
- Directed an in-depth analysis of cyber threat intelligence, identifying and mitigating over potential security breaches, significantly enhancing the organization's threat response capabilities using **firewall**, **SIEM** and **IDS/IPS** technologies.

### Software Engineer and Assistant Team Lead

March 2020 – September 2022

Strativ BD Limited | Dhaka, Bangladesh

- Orchestrated **unit testing** and **Java coding processes**, ensuring the adherence to project timelines and quality standards.
  - Effectively managed project responsibilities, driving success through **strategic planning** an efficient resource allocation.
- Conducted proactive research and development activities, staying abreast of industry trends to inform project decisions and maintain a competitive edge.

### Web Application Developer

February 2019 – January 2020

Saleduck Asia | Kuala Lumpur, Malaysia

- Enhanced system loading speed **3.2 times faster**, particularly beneficial in slower internet countries that achieved **Google Lighthouse** scores consistently exceeding 98%.
- Aced codebase transformation to the **MVC pattern**, resulting in **30% faster** development cycles and improved code maintainability.
- Implemented professional product management tools (**Bitbucket**, **Slack**, **Git**, **Docker**) to streamline **SDLC** processes.

## Notable Projects

### Implementing a SOC and Honeynet in Azure

Source: <https://github.com/mahin12/Honey-Net-Project>

Platforms and Technology Used: Azure Virtual Machine, Microsoft Sentinel (SIEM), Log Analytics

### Project: AI-Powered Security Vulnerability Detection in Source Code

Source: [github.com/mahin12/chatgpt\\_network\\_security](https://github.com/mahin12/chatgpt_network_security)

Platforms and Technology Used: Heroku Cloud Service, Flask, OpenAI's GPT 3.5 Turbo, MongoDB

## Skills

**Cybersecurity:** Vulnerability Assessment (Nessus), Threat Risk Assessments, Digital Forensics and Incident Response

**Programming:** Python, Java, React JS, jQuery, Version Control (GitHub), Docker

**Networking:** Network simulation, Cisco Packet Tracer, Routing, IP/TCP, Subnetting, Nmap, Searchploit

**Tools/Frameworks/IDEs:** Microsoft Office Suite, JIRA, Bitbucket, PyCharm, PhpStorm, Laravel, Bootstrap, Django

**Cloud Platforms/Databases:** Heroku, Netlify, MySQL, SQLite

**Systems:** Linux, MacOS, Windows, VirtualBox

**Other:** Data Visualization, Ethical Hacking, Excellent Communication