

# ATISHAY DIKSHIT

Los Angeles | 213-574-5102 | 8611 5524 | [atishayd@usc.edu](mailto:atishayd@usc.edu) | [atishaydikshit.com](http://atishaydikshit.com) | [linkedin.com/in/atishaydikshit](https://linkedin.com/in/atishaydikshit) | [github.com/atishayd](https://github.com/atishayd)

## EDUCATION

### University of Southern California

Los Angeles, California

Bachelor of Science in Economics and Data Science, Minor in Cybersecurity

May 2025

- **Teaching Assistant** for Accelerated Programming in Python (F23-S24)
- **Director of Curriculum** for Association of Innovative Marketing Consulting (AIM)

## SKILLS

**Relevant Coursework:** Software Engineering, Algorithms, Artificial Intelligence, Data Structures, Enterprise Network Design, Linear Algebra, Machine Learning, Econometrics, Natural Language Processing, Ethical Hacking, Computer Systems, OWASP Top 10

**Technical:** C++, Python, HTML, Java, HTML, CSS, PHP, R, SQL, Hadoop, Spark, Hive, NoSQL, MongoDB, AWS, Pandas, NumPy, TensorFlow, PyTorch, scikit-learn, Predictive Modeling, Penetration Testing, Kali Linux, Tableau, KAPE

## WORK EXPERIENCE

### Ernst & Young

Singapore

Cybersecurity Intern

May 2024-August 2024

- **Spearheaded two international ransomware investigations** as part of the Incident Response team, uncovering a **30% data exposure** through Axiom Magnet and X-Ways analysis; conducted in-depth **bash scripting, metadata, and file analysis** to reconstruct attacker activity, delivering executive-ready reports that enabled targeted threat containment and bolstered future breach defenses.
- **Collaborated with two cross-functional teams** to investigate PII from leaked documents by crafting complex SQL queries to trace sensitive data **across enterprise networks**, identifying critical exposure points and deploying advanced encryption and data protection measures that **reduced potential data loss by 70%**, securing over **100,000 sensitive records**.
- **Developed advanced Rubber Ducky payloads** coded in **DuckyScript** to simulate complex cyber-attack scenarios, including keystroke reflection, OS detection, and remote access—delivered live demonstrations to **over 110 stakeholders**.
- **Engagement** directly contributed to **increasing client cybersecurity resilience by 20%**, significantly **reducing data exposure risk** and **enhancing client confidence** in incident response protocols

### Ernst & Young

Singapore

Cybersecurity Consulting Intern

May 2023-August 2023

- **Configured a Python-based Nmap compiler**, leveraging **Pandas** and **Scapy** to process **complex Nmap scan files**; categorizing open ports, services, IP addresses, and protocols to assess vulnerabilities based on scan parameters, generating CSV reports **that improved analysis efficiency by 40%** and provided clear, actionable insights for cybersecurity teams
- **Led weekly client status updates** on vulnerability findings, leveraging Alteryx to automate data processing, filtering, and enrichment of Nmap scan outputs, and integrating **PowerBI visualizations** to highlight high-risk ports, protocols, and IP addresses, **expediting response times by 15%** to security threats.
- Engineered proactive **data protection solutions across fifteen environments**, **directly contributing to the system** integrity and strengthening cyber resilience.

### Can Mah!

Singapore

Software Engineer (Co-founder)

January 2020-December 2020

- Engineered an **automated, real-time digital grocery stock management platform** using **Python, HTML, PHP, and CSS**
- Implemented a **Firestore database** to manage high-frequency transactions, processing over **500 daily updates** and synchronizing user orders with digital stock levels to achieve **operational efficiency** and **real-time reliability**.
- **Collaborated** with the local **startup** GoodHood.sg to deploy Can Mah! as a **web API** integrated into their platform, extending COVID-19 risk mitigation services **to over 1,000 residents** with **real-time** access to essential resources
- Received **\$5,000** in grants from **Oscar Temasek** and a **further \$25,000** from various innovation **grant competitions**

## PROJECTS

**Phishing Detection AI:** Built an **LSTM-based phishing detection** model and deployed as a **Flask API**, utilizing **natural language processing (NLP)** and **TensorFlow** for sequence modeling to **classify email content** in real-time

**ChatDB:** Developed a **ChatGPT-like database query** assistant without using **large language models (LLMs)**, supporting both **SQL** and **NoSQL** databases through logic-driven **query generation** that enables users to learn how to explore database schemas and generate complex queries using constructs

**Optical Character Recognition:** Engineered a **C++-based OCR engine** for accurate detection and parsing of numeric characters across varied fonts, employing **advanced image processing**, digit segmentation, and blob analysis techniques, achieving **98% accuracy**.