

# Matthew Lee

## Cyber Security Engineer

Highly motivated, exceptional problem solving skills, personable, thrives in both team-based and independent environments, strong determination for personal development.

✉ mattdouglee@gmail.com

📞 631-935-2858

📄 mattplum.github.io

🌐 linkedin.com/in/mdlee12097

## EDUCATION

### Master of Science in Cyber Security

Grove School of Engineering, City College of New York

08/2021 - Present

Honors: Summa cum laude

### Bachelor of Science in Computer Information Systems

University of Delaware

08/2015 - 05/2019

## WORK EXPERIENCE

### Senior QA Engineer

Con Edison (Consultant)

08/2020 - 10/2021

Worked as a Consultant for Con Edison as part of their QA team per contract with RTTS

#### Achievements/Tasks

- Verified in-house suite of applications used by Con Edison. Executed manual, automation and API testing with DevOps integration for CI/CD.
- Used Azure DevOps to open and close variances within the application.
- Ran Postman requests to test API endpoints.

### QA Engineer

Real Time Technology Solutions (RTTS)

10/2019 - 08/2020

#### Achievements/Tasks

- Validated functional requirements in development cycles.
- Helped build an automation framework and automated functional tests using Selenium in Microsoft Visual Studio C#.
- Used SQL techniques such as nested select statements and aggregate functions to return desired queries.

### IT Engineer

ProHealth (TekSystems)

07/2019 - 10/2019

#### Achievements/Tasks

- Extensively performed log review of proprietary software records.
- Created Python scripts to aggregate the data and feed the logs into Excel for further review.

## SKILLS

Python

Java

C#

React

SQL

Windows

Ubuntu

macOS

Virtual Box

## ACADEMIC PROJECTS

### OpenAI Steganography

- Used OpenAI's DALL-E API to generate images to use for steganography.
- Used LSB encryption method for encoding a message into the generated image.
- Used Flask to convert the Python program into a user-friendly web application.

### Pet Camera Hack

- Hacked into my pet camera using code injection to obtain root access
- Converted the exploit into a Python script to easily inject code into the camera to run root commands

### Web Security

- Completed Codepath Capture the Flag (CTF) assignments of SQL injection, XSS attacks, cryptography, hashing, session hijacking, steganography, etc.
- Deployed MHN-Admin VM on Google Cloud to create Dionaea and Snort honeypots to capture IP attacks from around the world.

### Penetration Testing and Ethical Hacking - Remote Access Trojan (RAT) Project

- Configured Linux VMs to act as Attacker and Victim in a Server/Client environment.
- Created a remote access Trojan virus that executed a backdoor attack to gain access to the victims' files and trigger a keylogger program.

### Secure Cloud Computing

- Built a Google Docs clone application, packaged it into a container with Docker and deployed the application to the cloud with GCP.
- Created the design requirement document, implemented cloud reliability requirements and security using two-factor authentication.

## REFERENCES

As Per Request

## INTERESTS

Cyber Security

Programming

Front-end

Back-end