# Matthew Lee

MS Cyber Security

Results-driven recent graduate with an MS in Cybersecurity, BS in Information Systems, and two years of experience in IT. A detail-oriented professional with a proactive approach to problem-solving and a commitment to learning for professional growth.

matthewdouglee@gmail.com | 631-935-2858 | New York | mattplum.github.io

## EDUCATION

**Master of Science in Cyber Security**
Grove School of Engineering, City College of New York
*08/2021 - 06/2023* *Honors: Summa cum laude*

**Bachelor of Science in Computer Information Systems**
University of Delaware
*08/2015 - 05/2019* *Deans List*

## WORK EXPERIENCE

**Application Support Analyst**
Con Edison (Consultant)
*08/2020 - 10/2021*
*Served as a Consultant for Con Edison, collaborating with the QA team under a contract with RTTS.*

*Achievements/Tasks*

- Successfully performed manual, automated, and API testing with seamless integration into DevOps for CI/CD pipelines
- Utilizing a ticket resolution approach, I effectively identified and addressed critical issues within the application, including conducting vulnerability testing as part of the troubleshooting and resolution process

**Senior QA Engineer**
Real Time Technology Solutions (RTTS)
*10/2019 - 08/2020*

*Achievements/Tasks*

- Contributed to the development of a secure automation framework and implemented automated functional tests using Selenium in Microsoft Visual Studio with C#
- Utilized Jira and Azure DevOps to provide efficient IT support, ensuring effective ticket resolution and maintaining information assurance

**IT Support Engineer**
ProHealth (TekSystems)
*07/2019 - 10/2019*

*Achievements/Tasks*

- Developed a robust software process to ensure the ongoing maintenance of data integrity
- Created Python scripts to aggregate data and facilitate the integration of records into Excel for comprehensive analysis

## SKILLS

Security+ | Python | Java | C# | Burp Suite | Wireshark | Virtual Box | React | Flask | Windows | Linux | SQL | GCP | Azure

## ACADEMIC PROJECTS

### OpenAI Steganography

- Utilized OpenAI's DALL-E API to generate images for steganography purposes
- Employed the LSB (Least Significant Bit) encryption method to encode a message within the generated image
- Utilized Flask to transform the Python program into a user-friendly web application

### IoT Camera Hack

- Successfully completed analysis of security vulnerabilities in a pet camera system, including exploring code injection techniques to understand potential risks and enhance security measures.
- Utilized Python to successfully gain shell access to the IoT device through code injection.

### CodePath Cybersecurity Course

- Earned a Codepath Intermediate Cybersecurity Course Certificate, demonstrating proficiency in diverse cybersecurity domains including SQL injection, XSS attacks, cryptography, hashing, session hijacking, steganography, with completion of Capture the Flag (CTF) challenges
- Utilized Google Cloud to deploy the MHN-Admin VM, enabling the creation of Dionaea and Snort honeypots for capturing IP attacks from global sources

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

- Developed a simulated remote access Trojan (RAT) in Python that was designed to explore potential security vulnerabilities and understand the impact of backdoor attacks and keyloggers on victim systems
- Configured Linux VMs to simulate an Attacker and Victim within a Server/Client environment

## REFERENCES

Upon Request

## INTERESTS

Hackathons | Coding | Incident Response | Security Certifications | CTF Competitions