# Yash Suhas Shinde

yshinde1@binghamton.edu |+1 607-624-9047 |linkedin.com/in/shindeyash28

## Technical Activities

**JerseyCTF (Participant)** **New Jersey, USA**

- Solved different CTF challenges by finding hidden flags, using forensic investigation tools such as Autopsy and Forensic Toolkit
- Analyzed web server logs for anomalies and vulnerabilities to exploit them to reach the goal

**Homelab** **New York, USA**

- Designed a robust virtual network using tools such as pfSense and Suricata for experimentation with various network attacks, configuration of firewalls, and vulnerability scanning to mimic various real-world security scenarios.
- This will be extended to a home server setup using the NAS drive for efficient management of personal storage.

**CTF Club Member @SUNY Binghamton** **New York, USA**

- Engaged in solving CTF-related challenges in cryptography, reverse engineering, and digital forensics.
- Participated in team-based problem-solving sessions to enhance technical skills and practical knowledge in cybersecurity.

## Work Experience

**SUNY Binghamton** **New York, USA**
*Research Intern* July 2024 - Present

- Improved data security by deploying and configuring Passbolt on AWS, securing data access with SSL, and automated backups.
- Designed and managed a customized firewall, introducing advanced security features that helped enhance the understanding of network protection and access control.

**Trace Labs** **Vancouver, CA**
*Volunteer Coach* Nov 2024 - Present

- Mentored teams in Search Party CTFs, driving collaboration, and guiding participants in OSINT to find flags related to actual missing persons cases.
- Community impact is enhanced by support for intelligence vetting, learning of innovative approaches toward OSINT, and knowledge-sharing among participants with varied skills.

**TCRInnovation** **Mumbai, IN**
*Junior SOC Analyst* Apr 2022 - Aug 2022

- Investigated security incidents using Google Chronicle and Suricata, analyzing logs and network traffic to identify anomalies and mitigate potential threats.
- Conducted threat hunting and log analysis to detect suspicious activities, improving incident response efficiency and reducing investigation time.

## Certifications

- ISC2 Certified in Cybersecurity (ISC2) Dec 2024
- CompTIA Security+ SY0-701 (CompTIA) Aug 2024
- Google Cybersecurity Professional Certificate (Coursera) May 2024
- EntryLevel Virtual Experience Program for Data Analyst (EntryLevel) Aug 2021

## Projects

**Secure Election Booth** Sep 2023 - Mar 2024

- Designed an E.V. system with secure SSL encryption and one-time voting, hence enhancing voter anonymity and integrity through the elimination of unauthorized vote duplication.
- Implemented multi-threaded client-server communication to improve system responsiveness and reinforce security on the server through public-key certificate generation.

**Web Proxy Server** Aug 2022 - Nov 2022

- Designed a multithreaded web proxy server that supports caching and validation, reducing server response time by 25while maintaining data consistency with a 120-second cache expiration policy
- Improved reliability due to effective socket programming, the accuracy of data is higher, and the speed of retrieval of data is increased.

**Location of New Store Detection** Aug 2021 - Apr 2022

- Optimized database queries by 12%, thereby optimizing the whole backend processes and giving seamless experiences on the web interfaces.
- This paper was selected for technical presentation at the ICATM conference and reflects a valuable technical insight analysis into the project.

**Enterprise Network Design for College** Aug 2021 - Dec 2021

- Planned and developed a scalable and secure network infrastructure for a college, ensuring efficient IP assignment and centralized cloud storage to increase the reliability of the network by 40%.
- Reduced potential for downtime with a strategic network plan, high performance, and secure data access.

## Education

**SUNY Binghamton** May 2024
Masters in Computer Science
**University of Mumbai** May 2022
Bachelor of Engineering in Information Technology

## Skills

Incident Response — Security Monitoring — SIEM Solutions — Log Management — Vulnerability Management — OpenVAS — Suricata — Autopsy — FTK Imager — Ghidra — AWS — Azure — Python — Java — Networking — Access Control — Security Policies — Threat Analysis — OSINT — Firewall Configuration — Cryptography — Web Security — Data Security — Reverse Engineering — SOC