# Hyunjoon (Joon) Kim

Minneapolis, MN • kim00967@umn.edu • 612-757-3292 • www.linkedin.com/in/joonkim0625

## Objective

Cybersecurity professional with a Master's degree in Computer Science and hands-on experience in SOC operations, and IAM. Adept at using tools like Splunk, CrowdStrike, and Qualys to secure and optimize IT infrastructure. Seeking to leverage technical expertise and analytical skills in a challenging cybersecurity role.

## Education

**University of Minnesota, Twin Cities** **Minneapolis, MN**
*Master of Science in Computer Science, GPA: 3.71* *Sep 20201 – Dec 2023*

*Capstone Project*: Enhanced FuzzBALL's compatibility with modern Linux-based systems and integrated it with Ghidra for advanced binary analysis.

## Experience

**Cybersecurity Analyst, Minnesota Judicial Branch,** St. Paul, MN *Jan 2024 – Present*

- SOC (Security Operations Center)
  - Monitored and triaged suspicious network access events, such as unauthorized logins from outside the U.S. and excessive login attempts, using Splunk and CrowdStrike.
  - Automated the extraction and formatting of vulnerability management data from Qualys, streamlining the distribution process to various departments for review using Python and PowerShell scripts.
- IAM (Identity and Access Management)
  - Triaged 365 expired account activity cases, resolving 357, significantly reducing the number of lingering expired accounts in the system, and enhancing overall network security.
  - Utilized ADAudit+, MS Entra, and Splunk to monitor and address suspicious network activities, ensuring compliance with security protocols.
  - Maintained and optimized the use of Delinea Secret Server (PAM solution) and NetIQ (IAM software) by using Python and JavaScript to enhance internal security processes.
  - Conducted internal separation audits to verify the removal of credentials following HR separations, preventing unauthorized access.

**Cybersecurity Analyst Intern, Minnesota Judicial Branch,** St. Paul, MN *May 2023 – Aug 2023*

- Conducted security assessments on visitor kiosk computers at a City Service Center, identifying vulnerabilities and recommending mitigation measures in collaboration with a team of four
- Developed PowerShell and Bash scripts for automating tasks in extracting browser histories from a host computer and discovering default credentials on IoT device web interfaces
- Utilized EDR/SIEM tools like CrowdStrike, Splunk, and Qualys to monitor and respond to the latest threats and vulnerabilities across the organization's assets

**Graduate Teaching Assistant, University of Minnesota,** Minneapolis, MN *Sep 2021 – Dec 2023*

- Assisted in grading assignments/exams and held office hours for a class of 400 undergraduate students.

**Research Assistant, University of Minnesota,** Minneapolis, MN *May 2022 – Dec 2022*

- Assisted in running experiments to find the reachability problem in the AFLGo fuzzer
- Used afl-cov to extract code coverage information from applications that AFLGo was used
- Automated the process of running the fuzzer based on the target applications by creating scripts and Makefiles

## Skills / Certifications

- Programming/Scripting Languages: Python, PowerShell, C, Assembly, JavaScript
- Security Software: Splunk, CrowdStrike, Qualys, ADAudit+, MS Entra, Delinea Secret Server, NetIQ
- Security Tools: Burp Suite, Ghidra, Hydra, Kali Linux, Nmap, Wireshark
- CompTIA Security+ (Certification Number: COMP001022332395), Valid through Sep 2026

## Awards

- 2023 John T. Riedl Memorial Graduate Teaching Assistant Award