

# Sooraj Krishnamoorthy Manikandan

(416)-731-7539 | [joesooraj@gmail.com](mailto:joesooraj@gmail.com) | [linkedin.com/in/sooraj-krishnamoorthy-manikandan](https://linkedin.com/in/sooraj-krishnamoorthy-manikandan) | [soorajkm.vercel.app](https://soorajkm.vercel.app)

## EDUCATION

### McMaster University

Hamilton, ON

Bachelor of Applied Science in Computer Science, Minor in Business

Expected Graduation: May 2027

Honors: Dean's Honour List, Class of 1956 50th Anniversary Scholarship

## EXPERIENCE

### Cybersecurity Intern (Co-op)

May 2025 – Aug 2025

CGI Inc.

Hybrid

- Performed real-time monitoring and triage of security alerts using QRadar, identifying and escalating potential threats in alignment with standard operating procedures.
- Conducted first-level investigation by analyzing logs, filtering false positives, and classifying incidents to support efficient response.
- Documented alerts and incident details accurately, ensuring smooth handover to L2 analysts and maintaining compliance with SOC protocols.

## PROJECTS

### Python Host-Based IDS (HIDS) | Python, SHA-256

January 2026

- Developed a lightweight HIDS in Python to monitor system integrity and detect unauthorized file modifications in real-time.
- Implemented signature-based detection using SHA-256 hashing to alert on changes to critical system files and configuration directories.
- Integrated a logging mechanism to record timestamps and user details of suspicious activities for forensic audit trails.

### Virtual SOC Analyst Simulation | Splunk, TryHackMe

January 2026

- Engaging in high-fidelity security simulations to detect and triage real-world threats including **phishing**, **malvertising**, and **web-based attacks**.
- Utilizing **Splunk** (SIEM) to analyze log data, distinguish true threats from false positives, and reduce Mean Time to Respond (MTTR).
- Drafting detailed incident response case reports to document investigative findings and remediation steps, receiving automated feedback to refine reporting accuracy.

### Life-Link-Live | Full Stack Web

November 2025

- Designed and developed an emergency response web application to assist users during natural disasters such as earthquakes and tsunamis.
- Focused on rapid accessibility and clear user flows to help users quickly access critical information and emergency resources.

### MacFind | Frontend, UX Design

November 2025

- Developed a frontend-only lost and found web application for McMaster University users to post and browse lost or found items.
- Applied human-centered design principles and usability heuristics to create an intuitive and accessible interface.

### AuxiHelper | Cohere API, Google Cloud Vision

January 2025

- Designed and developed a platform that streamlines how users connect with service providers by interpreting user-reported problems and matching them with relevant solutions.
- Implemented AI-driven recommendations using Cohere APIs and Google Cloud Vision to analyze files and provide intelligent matching.

## CERTIFICATES & TECHNICAL SKILLS

**Certifications:** CyberStart Canada (Selected Participant), Career Essentials in Cybersecurity

**Languages:** Python, ELM, Haskell, C, Java, SQL, Javascript, HTML/CSS

**Libraries:** React.js, Node.js, NumPy, pandas, Matplotlib

**Tools:** Splunk, QRadar, Wireshark, MetaSploit, VirusTotal, PowerBI, Tableau, VS Code, Linux