Yu Heng Su

✉ yuhengsu.tw@gmail.com | in linkedin.com/in/yuhengsu | ☎ 289-983-5712

Experience

iG2 Group Inc. *August 2021 – Present*
Cyber Security Analyst and Developer | www.ig2.ca Toronto, ON

- 5+ years of experience leading incident response across the Microsoft Sentinel ecosystem including the development of custom KQL threat-hunting queries, automated SOAR workflows, and high-level Azure Workbooks
- Engineered unified endpoint security architectures by configuring integrated EDR/XDR solutions; optimized security posture through custom policy enforcement, attack surface reduction rules, and automated response actions to preemptively block malicious activities
- Served as the lead SOC Operator, performing incident investigations, conducting penetration testing, and automating the vulnerability lifecycle to ensure continuous endpoint compliance
- Managed and led technical touchpoints, delivered forensic reports, and conducted workshops to educate senior management and security analysts on platform optimization.
- Enforced Identity Management (IdM) and SASE frameworks, deploying Cisco Meraki (SD-WAN) and MFA policies to mitigate credential-based attacks and secure distributed environments.

Ministry of Education *April 2022 – Present*
Specialized IT Consultant Toronto, ON

- Managed complex technical projects, coordinating cross-functional IT teams across various departments to ensure the successful delivery of large-scale security initiatives.
- Assisted in the architectural design and strategic planning of an integrated cybersecurity operations model, leveraging identity security, SIEM, SOAR, and agentic AI to maximize organizational efficiency.
- Implemented SOC operations for clients from the ground up, including the configuration of Microsoft Sentinel, custom KQL detections, and Sentinel Workbooks.
- Engineered advanced security automation using Azure Logic Apps to develop SOAR playbooks; integrated third-party APIs to automate data enrichment and streamline multi-stage incident response workflows.
- Spearheaded the vulnerability life cycle management by deploying automated patch and vulnerability management tools to remediate endpoint exposures across multiple boards.
- Applied MITRE ATT&CK and NIST frameworks to incident detection and response workflows to standardize protocols and significantly harden the institutional security posture.
- Researched and developed basic agentic AI solutions leveraging DeepSeek, Azure APIs, and Google Vertex AI to automate incident categorization and investigation, significantly enhancing SOC operational efficiency.
- Developed and delivered technical workshops and educational materials to train security analysts on SOC operations, incident response methodologies, and the optimization of technical tool sets.
- Led technical cross-functional coordination between IT teams, managing vulnerability reporting via Power BI dashboards, and delivering specialized workshops to senior management and analysts.

University of Toronto *August 2020 – May 2021*
Full Stack Developer | cssc.utm.utoronto.ca Toronto, ON

- Engineered a suite of web-based educational tools using a combination of NodeJS, Nuxt and Vue.js to support over 1,000 students, focusing on improving resource accessibility and user engagement
- Developed dynamic back-end solutions and RESTful APIs using JavaScript to facilitate real-time data processing and interactive learning features across multiple platforms.
- Collaborated on the front-end architecture, implementing responsive design patterns for high-traffic resource pages and specialized student utility tools.
- Spearheaded repository management and version control for the CSSC website, ensuring code integrity and facilitating seamless team contributions via GitHub.
- Facilitated technical workshops focused on student success and software development fundamentals, bridging the gap between educational theory and practical application.

Education

University of Toronto *Sep 2017 – May 2021*
Bachelor of Science | Honours Computer Science and Mathematics Toronto, ON