

Jeffrey Beh

<https://www.linkedin.com/in/jeffreybeh/>

<http://www.github.com/Jeffiftyone>

Email : resume@jeffbeh.com

Mobile : (647) 839-0113

SKILLS

- **Security Tools & Platforms:** Wireshark, Splunk (basic), TryHackMe, Nmap, OSINT, Git, Power BI, Postman
- **Languages:** SQL, JavaScript, Python, HTML, CSS
- **Key Technical Strengths:** Log analysis, network traffic analysis, data querying, REST API development, version control, teamwork

EDUCATION

- **University of Toronto School of Continuing Studies** Toronto, ON
Full Stack Coding Boot Camp Graduated 2022
- **York University** Toronto, ON
Bachelors of Arts in Information Technology (with Honours) Graduated 2021

WORK EXPERIENCE

- **Peropyx**
Data Analyst and Data Evaluator May 2023 - current
 - **Analytics:** Wrote and optimized SQL queries to extract, filter, and aggregate data, supporting analytics and improving reporting efficiency.
 - **Data Verification and Cleaning:** Verified and enhanced AI-gathered data by leveraging OSINT tools and Google Dorking, improving information accuracy and relevance. Cleaned and pre-processed large datasets to eliminate errors and inconsistencies, ensuring quality data for decision making.
 - **Visualization:** Built data dashboards and visualizations in Power BI, translating complex data into actionable insights for stakeholders.
- **Poke Guys (Restaurant)** Markham, ON
Supervisor, Management Team Apr 2018 - Mar 2023
 - **Onboard Training:** Trained and onboarded 20+ new hires and supervisors, improving onboarding consistency and retention by 25% .
 - **Interpersonal skills:** Resolved customer issues through active listening and situational analysis, leading to increased customer satisfaction and loyalty.
 - **Communication:** Communicated team performance metrics and process improvements to upper management, improving operational efficiency.

CYBER SECURITY PROJECTS & LABS

- **OC Fundamentals Lab**
TryHackMe Blue Team Path (Ongoing)
 - **Log Analysis:** Analyzed logs and triaged simulated security incidents using SIEM-style platforms, gaining hands-on experience in alert detection and SOC workflows.
- **Packet Analysis**
Wireshark
 - **Network Monitoring:** Captured and dissected network traffic to identify anomalies, such as malformed DNS queries and suspicious payloads, improving detection skills.
- **Log Ingestion & Detection**
Splunk (Self-Study)
 - **Threat Detection:** Built log search queries, visualized patterns through dashboards, and created basic alerts to monitor potential threats in system data.

CERTIFICATIONS & TRAINING

- **CompTIA Security Plus:** In Progress
- **Google Cybersecurity Certificate:** Planned
- **Splunk Core Certified User:** Planned