IHAR GANCHARENKA

Cybersecurity Analyst & Developer

[LinkedIn](#) | [GitHub](#) | [Personal Portfolio](#) | igorganch1@gmail.com | 647-787-0734 | Toronto, Canada

---

An IT professional with a background in software development and knowledge of cybersecurity. Skilled in analyzing and solving complex problems with a dedicated approach. Aiming to leverage my analytical thinking and problem solving skills to contribute to your company's digital assets.

TECHNICAL SKILLS

Languages: JavaScript, TypeScript, Java, C#, C++, C, Python, BASH, PowerShell, PHP, SQL, HTML, CSS

Frameworks: React, Angular, Node.js, Express.js, ASP.NET Core, ASP.NET, Django, Spring Boot, JQuery

Tools: SailPoint 7.x, SailPoint 8.x, Metasploit, Nmap, NetCat, Wireshark, VMWare, Splunk, Burp Suite, Docker, Kubernetes, AWS SDK, MongoDB, PostgreSQL, OracleSQL, MySQL, MSSQL, Entity Framework, OpenGL, Bootstrap, IDS/IPS

Methodologies: OOP, MVC, REST api's, SDLC, MITRE ATT&CK, STIX, CAR, Scrum, Sprint, Data Structures and Algorithms

Operating Systems: Linux/Unix, Kali Linux, Ubuntu, CentOS, RedHat, Windows

QUALIFICATION OVERVIEW

- Software development experience gained through internship; able to work with cutting edge technologies
- Strong Object Oriented Programming, Data Structures & Algorithms concepts gained through academics
- Experienced in developing and designing relational databases
- Excellent problem solving and debugging abilities obtained from troubleshooting code and Unix/Linux systems
- Proficient knowledge on networking and cloud as well as security and hardening best practices
- Experienced working with IAM software e.g SailPoint; able to set up policies, rules, entitlements, certifications, etc.
- Proficient in working with real-time data, performing log analysis, and detecting threats
- Able to quickly adapt to new situations; able to work independently and within a team

EXPERIENCE

Threat Intelligence Analyst, *Iron Defense Security Corporation*, Toronto   **January 2024 - Present**

- Spearheaded the development and operationalization of threat intelligence processes to identify, assess, and mitigate cyber threats in real-time, reducing potential security breaches by 30%
- Integrated threat intelligence with existing security solutions, such as SIEM, firewalls, and intrusion detection systems to enhance the cybersecurity posture of over 30 companies
- Conducted in-depth analysis of threat landscapes, including malware analysis and phishing campaigns, contributing to effective defensive strategies that protected organizations critical digital assets
- Utilized advanced analytical tools and methodologies, such as STIX, TAXII for sharing and consuming threat intelligence improving the overall speed and accuracy of response to cyber incidents
- Implemented advanced malware detection using AI, improving threat detection speed and accuracy by 15%

Full Stack Developer Intern, *Kiuloper*, Mississauga   **January 2022 - April 2022**

- Successfully redeveloped a full-stack web application overhaul for a high-profile client using CSS, HTML, JavaScript, JQuery, DOM, PHP, and React for clients, resulting in a 40% increase in user engagement
- Proficiently created API routes utilizing Node.js, Express.js, and optimized AWS MySQL queries which resulted a 20% improvement in page load times
- Conducted thorough unit testing and integration testing to identify and resolve software bugs, optimizing application stability and user experience

EDUCATION

Seneca Polytechnic   **September 2023 - April 2024**
Cybersecurity and Threat Management, *Graduate Certificate*

Seneca Polytechnic   **September 2018 - April 2022**
Computer Programming and Analysis, *Advanced Diploma*