LOGAN POORAN

Cybersecurity Student

CONTACT

Phone: (425) 233-4350

Email: Logan.pooran@gmail.com

Location: Lake Stevens, WA

EDUCATION

Lake Stevens High School
High School Diploma

Everett Community College
Associate of Science: Computer Science

Washington State University-Everett
Bachelor of Science: Cybersecurity
GPA: 3.85
Expected Graduation: May 2027

CLUBS

- Cybersecurity Club Vice President
- Association for Computing Machinery Treasurer

SKILLS

- Strong foundation in object oriented programming, software engineering principles, and modular design.
- Proficient in Java, C#, Python
- Knowledgeable in Data Structures and Algorithms
- Understanding of Computer Architecture
- Proficient in using Wireshark for packet analysis, Nmap for network scanning, and Tenable for vulnerability scanning.
- Familiar with Git/GitHub for collaborative development

CERTIFICATIONS

ISC2 Certified in Cybersecurity (Dec 2025)

PROJECTS

I.T. POLICY MODERNIZATION -SENIOR CAPSTONE PROJECT:
• Reviewing and assessing Snohomish County's public IT policies to identify gaps, outdated language, and improvement areas.
• Performing comparative analysis against peer municipalities using NIST Cybersecurity Framework guidance and public data.
• Delivering final report and briefing to County IT leadership highlighting proposed policy changes and implementation priorities.

YOUTUBE DATA ANALYZER -BIG DATA PROJECT:
• Developed a scalable YouTube Data Analyzer supported by a MongoDB backend and Apache Spark for performing large scale data analytics.
• Engineered advanced data query capabilities, including Top K which include rating and popular videos, and Range Queries which include size and duration over the large media dataset.
• Applied optimization techniques to accelerate algorithm performance and ensure the platform handles big data volumes effectively

MACHINE LEARNING FOR THREAT DETECTION - MACHINE LEARNING PROJECT:
• Designed and implemented a machine learning framework for cybersecurity threat detection using static binary and network based analysis of malware samples
• Integrated and preprocessed data from three distinct, large scale datasets: EMBER2024, Microsoft Malware Classification Challenge, and NSL-KDD to enable hybrid feature analysis
• Trained, evaluated, and compared 10 ML/Deep Learning algorithms to accurately classify malicious and benign activities.
•Applied advanced optimization techniques, including hyperparameter tuning and feature selection, to maximize model performance. Evaluated models using the key metrics: accuracy, F1 score and ROC/AUC.