


# BENJAMIN ALEXANDER

System Administrator  
& Cybersecurity Professional

425-786-3569 

benalexander2020@gmail.com 

Woodinville, WA 

<http://linkedin.com/in/benjamin-alexander2020/> 

<https://github.com/RaphaelAlexander> 

## WORK EXPERIENCE

### Whatcom

#### Transportation Authority

April 2025 - June 2025

#### Systems Administrator Intern

- Resolved **tier 1 and Level 2 helpdesk tickets**, resolving 20+ tickets weekly and using proper escalation procedures, while maintaining smooth operation of multi-user computer systems
- Managed systems security administration** functions, including creating user profiles and accounts for company of 100+ employees
- Administered Active Directory, Microsoft O365, and LANs**, and maintenance of physical/digital IT assets

### Make.Shift Art Space

March 2024 - September 2024

#### IT & Marketing Intern

- Worked directly with **OSI physical and network layers**, including installations, cable networking, and configuring routers/switches with HP Aruba networking.
- Work with **SQL database to analyze sales data**, develop marketing strategies, and facilitate with marketing team for deployment
- Development of Powershell** scripts to automate systems and user administration, including **group policy managements** and application settings changes

### Hammerhead Coffee Roasters

March 2023 - Present

#### Coffee Roaster

- Worked with a core team to deliver **excellent customer service** in a high paced environment. Built a community of baristas and regulars alike that carry on today.
- Growth mindset** added to company to constantly improve product quality and sales

## EDUCATION AND PROJECTS

### Whatcom Community College

### Western Washington University

### Google

#### SOC Analysis Lab

Designed and deployed a honeypot virtual machine on **Microsoft Azure** to attract threat actors, analyzing failed login attempts from global sources using KQL queries and geolocation mapping. Identified successful breach patterns including automated brute force attacks and privilege escalation techniques through **comprehensive log analysis**. Demonstrated **proficiency in threat intelligence, incident response, and security monitoring** by tracking attacker methodologies and system vulnerabilities to enhance understanding of cybersecurity defense strategies.

#### Programming & Automation

**Java and Python proficiency** to create flexible applications, interactive programs, and maximizing time efficiency with data structures. **Strong ability with Powershell and Bash** to automate user administration within a network. **Experience with MySQL** to retrieve, modify, and create information within large database systems. Create easy access to info and apply information to the real world

### Cybersecurity - Associates of Applied Science

### English - Bachelors of Arts

### Cybersecurity Professional Certificate

## SKILLS AND ACCOMPLISHMENTS

**Operating Systems:** Windows Server 2016/2019, Windows 10/11, Ubuntu, RHEL, Kali Linux

**Security Tools:** Wireshark, Snort, NMAP, Burp Suite, Splunk, Azure SIEM, KQL

**Programming/Scripting:** PowerShell, Python, Java, SQL, Bash

**Networking:** HP Aruba, Cisco, TCP/IP, OSI Model, DHCP, SSL/TLS, VPNs

**Cloud Platforms:** Microsoft Azure, Google Cloud Platform

**Directory Services:** Active Directory, Microsoft O365

**Pacific Rim Collegiate Cyber  
Defense Competition  
Team Competitor  
Network Defense & Incident  
Response - 2025**