Aslam Bwanika

Tacoma, WA | (253) 248-5457 | aslambwanika1@gmail.com | GitHub

Education

Saint Martin's University Lacey, WA

B.S. in Computer Science; Concentration in Cybersecurity & Cloud Computing *December 2025*

- **Relevant Coursework:** Cloud Computing, Network Security, Computer Security, Ethical Hacking, Operating Systems, Data Structures & Algorithms.

Technical Skills & Certifications

Languages: Python, Bash, SQL
AppSec & Security: Vulnerability Assessment, SIEM Monitoring, Incident Triage, Threat Detection, IAM/RBAC, Least Privilege, Security Documentation
Cloud & DevSecOps: Azure, AWS, GitHub Actions, CI/CD, Azure Monitor, Log Analytics
Tools & Frameworks: Microsoft Sentinel, KQL, Tenable, Splunk, Wireshark, Linux (Ubuntu, Kali), Flask, Git/GitHub, Jenkins, pytest, Bandit, pip-audit
Network & Systems: TCP/IP, DNS, Firewalls, Packet Analysis, Network Troubleshooting, VPN, IDS/IPS
Certifications: Security Plus (Expected December 2026)

Experience

Saint Martin's University Lacey, WA

IT Intern *Dec 2021 – Dec 2025*

- Provided Tier 1 technical support to students, faculty, and staff, troubleshooting hardware, software, network connectivity, and account access issues.
- Supported identity and access management (IAM) operations, including password resets, account authentication, and multi-factor authentication (MFA) troubleshooting.

Washington State Gambling Commission Lacey, WA

Cloud Security Intern *Dec 2024 – May 2025, Aug 2025 – Jan 2026*

- Conducted vulnerability assessments across 300+ endpoints using Tenable Nessus, triaging high and critical vulnerabilities and coordinating remediation efforts to reduce organizational risk.
- Performed application security reviews for a $10M cloud migration, identifying hardcoded secrets and insecure coding practices prior to production deployment.
- Analyzed phishing metrics from **100+ employee** simulations to identify behavioral trends; designed targeted **awareness training** that reduced click-through rates by **90%.**

Youth Maritime Collaborative

Security Analyst Intern *Jun 2023 – Aug 2023*

- Conducted Tenable vulnerability scans on Linux servers and developed Python remediation scripts, improving compliance-monitoring coverage by **35%**.
- Implemented SQL role-based access controls (RBAC), performed access audits, and strengthened security configurations for applications and databases.

Microsoft

Engineering Tech Intern, AI Security & Data Integrity *Jul 2022 – Aug 2022*

- Developed Python automation for AI voice-data processing and validation across **100+** datasets, helping reduce data inconsistencies by **20%**.
- Supported security code reviews involving encryption and access control; integrated auditing into Azure CI/CD workflows using GitHub Actions and Jenkins.

Projects

Azure Cloud Security Monitoring & Detection Platform 2026

- Configured Azure Log Analytics and Azure Activity Logs ingestion for Microsoft Sentinel; verified AzureActivity event telemetry through KQL investigations.
- Built a read-only Python/Flask security dashboard, log collector, and detection logic for failed operations, RBAC changes, and sensitive resource updates; authored **four KQL queries**.
- Automated pytest, Bandit, and pip-audit checks via GitHub Actions; initial CI validation passed **7 tests** with no Bandit findings or known dependency vulnerabilities. Live Sentinel rule deployment remains under validation.

AWS Cloud Detection & Response Platform Aug 2026 – Present

- Built an event-driven AWS security platform using GuardDuty, IAM Access Analyzer, EventBridge, Lambda, and Terraform to detect, investigate, and automatically remediate high-risk IAM, EC2, and S3 security findings.