

Nathan Lim

253-389-6820 | contact@nathanlim.io | <https://nathanlim.io> | Seattle, WA
LinkedIn: [linkedin.com/in/nathanlimuw](https://www.linkedin.com/in/nathanlimuw) | GitHub: <https://github.com/nathan-hayashi>

PROFESSIONAL SUMMARY

Cybersecurity & IT professional with hands-on Identity & Access Management (IAM), endpoint hardening, and enterprise helpdesk experience. Current focus on enterprise IAM platforms (Azure, Sailpoint), passwordless authentication (CLEAR1), MFA (YubiKey/biometric), and PowerShell automation to reduce manual toil and improve security outcomes. CompTIA Security+ & AWS SAA certified & B.A. in MIS from UW Bothell.

EXPERIENCE

T-Mobile | Cybersecurity IAM Analyst November 2025 - Present

- Developed **PowerShell** automations and **Power Automate** reporting solutions for identity searches, access queries, and IAM workflows, reducing manual processing time by **75%** and generating actionable metrics via **PowerBI** dashboards
- Administered **CLEAR1** passwordless authentication systems for global workforce across acquisitions, mergers, retail, and contract operations, investigating and resolving **10000+** verification errors while maintaining **98%** automation rate
- Configure and maintain **Zscaler** VPN access controls through **Entra** ID permissions, troubleshooting VPN issues and investigating **CyberArk** key authentication problems to ensure secure remote access compliance
- Streamline queued user cases in regards to identity lifecycle tasks through **Power Automate** automation

T-Mobile | Cybersecurity Production Analyst July 2025 - November 2025

- Manage enterprise IAM operations across **Sailpoint**, **Workday**, **Jira**, and **Salesforce**, platforms, coordinating with principal engineers and API development teams to resolve platform bugs and enhance authentication workflows for global user base
- Collaborated with cybersecurity engineers and SOC analysts through **ServiceNow workflows**, documenting and escalating critical security vulnerabilities while implementing access control remediation strategies
- Created comprehensive documentation guides standardizing identity security practices across multiple workforce categories, reducing onboarding errors by **90%**
- Monitored user behavioral patterns and social engineering attack vectors, identifying and mitigating security threats through proactive threat intelligence analysis

Applied Physics Laboratory (UW) | IT Technician Support Specialist September 2023 - June 2025

- Obtained **DOD CUI clearance** for patching **100+** end users' **FortiClient Endpoint** CVE vulnerabilities, performing passive scanning to identify and remediate security weaknesses aligned with **ISO 27001** compliance standards
- Troubleshooted **800+** Level 1-3 end-user tickets including password resets, hardware diagnostics, system imaging, application deployment, and network analysis utilizing **Wireshark** and remote support tools
- Developed **PowerShell automation** scripts for user provisioning, system deployment, log aggregation, and security patching to streamline repetitive IT tasks
- Configured **150+** technical hardware systems and **450+ Active Directory** user credentials across Linux, Windows 10/11, and macOS environments utilizing PowerShell automation scripts for Windows imaging and deployment

EDUCATION

University of Washington, Bothell - BA in Management Information Systems June 2025

Certifications: CompTIA Security+ (SY0-701) 2025 | AWS Solutions Architect Associate (SAA-C03) 2026

TECHNICAL SKILLS

VScode | GitHub | Powershell | CLEAR1 | Identity Governance | Networking | AWS | Azure | RBAC | SSO | IAM