

JAWAD NAIMI

Aspiring Cybersecurity Specialist

253-329-9819



WORK.JAWAD.NAIMI@GMAIL.COM



Greater Seattle, WA



SUMMARY

Dynamic and results-driven professional with a rich blend of experience in cybersecurity, IT, and corporate security operations. Skilled at leading teams, mentoring colleagues, and streamlining workflows to exceed client expectations. Adept in leveraging tools like Power BI, SQL, and SailPoint to deliver actionable insights, strengthen access controls, and resolve security vulnerabilities.

Passionate about safeguarding systems and data, I thrive on tackling complex challenges, managing global operations, and fostering secure, efficient environments. With a focus on innovation and collaboration, I'm committed to driving impactful results and ensuring organizational safety and success.

EDUCATION

Southern New Hampshire University

Bachelor of Science in Cybersecurity
Present

Green River College, Auburn, WA

Associate in Applied Science-Transfer (AAS-T)
in Information Technology-Cybersecurity and
Networking

Year Up Puget Sound, Seattle, WA

Technical training & career development
program including college-level courses and a
six-month internship

Mili University Kabul, Afghanistan

Bachelor of Science in Law and political
science.

CERTIFICATIONS

- **Google Cybersecurity**
 - Foundation of Cybersecurity
 - Play it Safe: Manage Security Risk
 - Connect and Protect: Networks and Network Security
 - Tools of the Trade: Linux and SQL
 - Assets, Threats, and Vulnerabilities
 - Sound the Alarm: Detection and Response
 - Automate Cybersecurity Tasks with Python

PROFESSIONAL EXPERIENCE

Badge Tech II

Amazon Corporate Security Badge Office, Seattle, WA Oct 2023 – Current

- Directly managed and led a team of 20+ personnel, overseeing daily operations, task allocation, and performance evaluation while driving continuous improvement.
- Developed team competencies through hands-on mentoring and training, ensuring mastery of core processes and systems.
- Managed Physical Access Control Systems (PACS) ensuring secure facility access for 100+ corporate employees daily.
- Analyzed badge activity patterns and access logs to identify security anomalies, leading incident investigations and escalations.
- Validated and processed access authorization requests while maintaining strict security compliance protocols.
- Managed end-to-end employee credential lifecycle, implementing least-privilege access policies and maintaining accurate system records.
- Partnered with global security teams to resolve complex access management issues, ensuring 24/7 operational continuity.
- Delivered on-site technical support for badge-related issues while maintaining confidentiality of sensitive employee data.
- Developed and maintained standard operating procedures for badge management, ensuring alignment with security policies.

SKILLS

- Strong organizational and time-management skills
- Exceptional communication and interpersonal skills
- Ability to work independently and as part of a team
- Detail-oriented and able to handle multiple tasks simultaneously
- Experience in managing databases, and Company Assets.

REFERENCE

- Available upon Request

Cybersecurity Engineer Intern

Providence Health and Services, Seattle, WA

April 2023 – Sep 2023

- Configured and managed Workday Security, including domain security policies, business process security, and role-based access controls (RBAC) to ensure secure and compliant access to HR, payroll, and financial modules.
- Designed and implemented a KPI/KRI reporting dashboard using Power BI, delivering actionable insights to enhance security performance monitoring and executive decision-making.
- Conducted audits of Workday user access logs and sign-on activities, proactively identifying and mitigating unauthorized access risks while maintaining documentation for compliance.
- Strengthened identity and access management (IAM) protocols using SailPoint, integrating solutions with Workday to streamline user provisioning and deprovisioning processes.
- Analyzed SQL databases for potential vulnerabilities, supported incident response via ServiceNow, and conducted malware threat detection to ensure robust system security.
- Collaborated with stakeholders to define Workday business processes, develop functional security requirements, and design customized security roles tailored to organizational needs.
- Supported Workday updates by testing security configurations, validating new features, and updating user roles to align with evolving compliance standards.
- Created detailed documentation and conducted end-user training for Workday IAM workflows, improving system usability and adherence to security policies.

Badge Tech I

Amazon Corporate Security Badge Office, Seattle, WA April 2021– April 2023

- Assisted 100+ corporate employees and associates to resolve their badging issues via phone using Amazon Connect, email, trouble ticketing, and in-person through a Walk-Up service.
- Utilized 10+ computer systems and databases to verify status of 50+ employees to ensure workplace safety.
- Authenticated valid authorization and handling various requests for credentials as necessary.
- Processed all incoming materials and updated databases with current information for the Walk-Up offices.