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
Currenlty in progress.

Green River College, Auburn, WA

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

Year Up / Seattle Central College, Seattle, WA

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

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.

PROFESSIONAL EXPERIENCE

Badge Tech II

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

- Lead the team by assigning tasks, overseeing assignments, and providing feedback to ensure all client requirements are met while mentoring new employees on processes and systems.

- Manage physical access control systems (PACS) to ensure secure entry for over 100+ corporate employees daily, maintaining the integrity of workplace security.

- Monitor and analyze badge activity logs to identify unusual access patterns and escalate potential security breaches to the appropriate teams for investigation.

- Authenticate valid authorization for access requests, ensuring compliance with security protocols and mitigating unauthorized access risks.

- Assist in the provisioning and deprovisioning of employee credentials, following security policies for least-privilege access, and ensuring all updates are logged accurately in the system.

- Collaborate with global security teams to troubleshoot and resolve complex badge-related issues, maintaining operational efficiency and secure access management.

- Provide on-site assistance to employees experiencing badge or access issues, while adhering to company security protocols and safeguarding sensitive employee data.

- Document procedures for badge issue resolution, ensuring compliance with company-wide security and operational policies.

CERTIFICATIONS

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

REFERENCE

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.