Employment Opportunity

Quil Ceda Village
qʷəl'sidəʔ ʔalʔaltəd

8802 27th Ave NE, Quil Ceda Village, WA 98271
Office: 360-716-5000 • www.QuilCedaVillage.org

JOB TITLE: Cybersecurity Analyst

DEPARTMENT: Tulalip Data Services

PAY RANGE: $41.87 - $62.80

JOB DESCRIPTION SUMMARY:

The Cybersecurity Analyst supports the protection of Tulalip Data Services' information systems, networks, applications, and data by monitoring security events, investigating potential threats, assisting with incident response, and supporting vulnerability management activities. This position helps implement and maintain security controls, document security and audit evidence, support compliance with applicable policies and regulatory requirements, and collaborate with IT staff to reduce cybersecurity risk across the organization.

TO APPLY: Complete the web form application located on the Quil Ceda Village Self-Service portal: https://quilcedavillagewa.munisselfservice.com/ess/EmploymentOpportunities. For more information or questions, please visit http://quilcedavillage.org/Employment or call Quil Ceda Village Human Resources at (360) 716-5017.

NOTE: The Tulalip Tribes publicly announces that Indian Preference in hiring applies to Tulalip job opportunities.

EMPLOYEE CLASSIFICATION: Exempt

EMPLOYEE REPORTS TO: IT Director or designee

EMPLOYEE SUPERVISES: [None]

EDUCATION AND CERTIFICATION:

- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (required).
- Associate degree in a related field with relevant experience may be considered.
- An equivalent combination of education, certification, and progressively responsible experience may be substituted for degree requirements.
- CompTIA Security+ or equivalent cybersecurity certification required within a timeframe established by management.
- SSCP, Microsoft Security certifications, CEH, CySA+, GSEC, or other relevant cybersecurity certification preferred.

KNOWLEDGE OF:

- Cybersecurity frameworks and standards, including NIST and ISO 27001
- Identity and access management principles and security controls.
- Network infrastructure, server environments, systems administration, and network monitoring software.
- Vulnerability assessment methodologies and risk management practices.
- Security auditing principles and documentation requirements.
- Current cybersecurity tools, technologies, and threat mitigation strategies.
- Applicable laws, regulations, and compliance requirements, including HIPAA, PCI-DSS, NIST, and CJIS.
- Data protection methods and security best practices.

SKILLS IN:

- Monitoring and analyzing security events using SIEM, endpoint detection, vulnerability management, and related cybersecurity tools.
- Supporting firewalls, VPNs, IDS/IPS, endpoint protection, and secure configuration practices.
- Performing vulnerability scanning, control validation, and remediation tracking.
- Developing basic scripts or automation using PowerShell, Python, Bash, or similar tools.
- Supporting Microsoft 365, Azure, Microsoft Defender, Intune, and Entra ID security controls.
- Analyzing complex security issues, documenting findings, and recommending practical risk-based solutions.

ABILITY TO:

- Work independently and collaboratively in a team environment.
- Communicate effectively with technical and non-technical stakeholders.
- Organize, prioritize, and manage multiple assignments.
- Exercise sound judgment when responding to security events.
- Maintain confidentiality and handle sensitive information appropriately.
- Produce accurate and detailed documentation.

EXPERIENCE:

- Three (3) years of progressively responsible experience in cybersecurity, information security, or a closely related information technology role.
- Preferred experience with security monitoring, incident response, vulnerability management, phishing investigations, Microsoft Defender, Microsoft Sentinel, Entra ID, and security compliance activities

- Experience in regulated environments subject to CJIS, HIPAA, or PCI-DSS requirements.
- Experience with security monitoring, incident response, governance, risk, and compliance (GRC) programs.
- Experience responding to security incidents and conducting forensic investigations preferred.
- Experience with vulnerability management and security assessment tools preferred

OTHER REQUIREMENTS:

- Required to use company vehicle(s) to visit various customer locations as well as the Tribal departments in the conduct of required duties
- Must have the tolerance and patience for dealing with upset, angry, and/or frustrated individuals.
- Must maintain any required certifications throughout employment.
- Must have and maintain a valid state driver's license.
- Must possess and maintain personal automobile insurance
- Must be able to complete a Tribal, State, and Federal background investigation.
- Must be able to pass a hiring and periodic random urinalysis.
- Must be willing to attend progressive job-related training as requested.
- Must have a successful employment history with current and past employers.

PHYSICAL CHARACTERISTICS AND/OR PREREQUISITES:

- Manual and finger dexterity for the operation of a personal computer and routine paperwork.
- Stamina to sit, stand, and/or walk for prolonged periods of time.
- Tolerance to be exposed to a computer screen for prolonged periods of time regularly.
- Ability to occasionally lift, carry, move, or position computer equipment, peripherals, and related materials weighing up to 25 pounds.
- Mobility to bend, stoop, and/or climb stairs on an occasional basis.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

- Monitor systems, networks, and security alerts for potential threats and vulnerabilities.
- Triage security alerts and incidents, determine severity, document findings, and escalate issues in accordance with established incident response procedures.
- Investigate, document, and respond to cybersecurity incidents.
- Assist with cybersecurity risk assessments, security reviews, and risk remediation activities to reduce organizational risk.
- Perform vulnerability assessments and coordinate remediation activities.

- Monitor and support cybersecurity technologies and security controls, escalating platform configuration or engineering issues as appropriate.
- Assist in developing, implementing, and maintaining cybersecurity policies, standards, and procedures.
- Collaborate with IT staff and business units to ensure secure system configurations and practices.
- Maintain security, audit, and incident response documentation.
- Participate in security awareness, compliance, and risk management activities.
- Research emerging threats, vulnerabilities, and cybersecurity trends.
- Support periodic access reviews, privileged access reviews, and account security documentation.
- Assist with preparing cybersecurity evidence for audits, compliance reviews, and internal assessments.
- Track remediation activities related to vulnerabilities, security findings, and risk treatment plans.
- Assist with phishing awareness, cybersecurity training, and user security communications
- Document incident timelines, response actions, lessons learned, and corrective actions.

TERMS OF EMPLOYMENT:

This regular full-time position requires at least 40 hours per week or 2,080 hours per year. Employees may be required to work outside regular business hours, including weekends, special events, or on-call assignments. After completing the applicable probationary period, employees may be eligible for a pay increase, subject to budgetary restrictions. This position requires on-site work; telecommuting and relocation assistance are not provided.

Disclaimer: This job description describes the general nature and level of work performed by employees in this position. It is not intended to be a complete list of all duties, responsibilities, qualifications, or working conditions. Management reserves the right to add, modify, remove, or designate essential job functions at any time. This job description is not an employment agreement or contract.