Town of Oro Valley Classification Description

Title: Cybersecurity Analyst
Job Code: 1530
FLSA Status: Exempt
Department: Innovation & Technology
Salary Grade: 260

POSITION SUMMARY:

Under general supervision of the Network Manager, the Cyber Security Analyst is responsible for researching, implementing, and maintaining cybersecurity systems and solutions. This includes implementing policies, standards, baselines, guidelines, and procedures as well as conducting vulnerability audits and assessments. The incumbent is expected to be knowledgeable of the enterprise's security goals, policies, procedures, regulatory requirements, and guidelines, including actively working towards upholding those principles.

ESSENTIAL JOB FUNCTIONS:

- Evaluates, recommends, implements, and monitors IT security measures and programs in accordance with Town policies, procedures, IT security standards, new attacks, and threat vectors.
- Secures and monitors all systems (application and infrastructure) including access control systems, financial systems, CJIS, business intelligence, confidential, and customer service systems.
- Responds to and resolves incidents, providing guidance to all levels of the organization; may serve as technical lead on incidents.
- Remediates incidents found in audits, reports, and analysis. May work with law enforcement and vendors to manage security threats.
- Supports information security effectiveness by evaluating the results of, and developing action plans, for vulnerability assessments, penetration testing, process, and policy audits.
- Develops dashboards and or reports to provide awareness, training, and status information to other staff. Communicates information clearly, effectively, and as appropriate to the audience.
- Maintains clear and concise documentation; documents incident management activities, (e.g., time spent, actions taken, and status of incident); assists in designing and documenting cybersecurity or privacy processes, procedures, and standards.

- Selects appropriate exercises from partner agencies (i.e. State of Arizona, Arizona National Guard) and improves Town security based on findings.
- Researches the latest information technology security trends and recommends security enhancements.
- Resolves problems through internal resources or through consultation with vendor technical support staff.
- Assists in the development of security policies, standards, and best practices; develops and recommends compliance strategies for IT security programs, assesses risks of noncompliance with IT security policies, standards, and guidelines and reports findings.
- Develops, implements, and evaluates security awareness training programs and trains staff on security protocols, policies, and procedures.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:

- Knowledge of enterprise information security architecture, design, and engineering with a primary focus on technologies, tools, and solutions
- Knowledge of incident response, security information event management, intrusion detection systems, threat hunting
- Knowledge of endpoint protection and response, and security orchestration automation and response
- Knowledge of vulnerability scanning tools.
- Ability to perform trend analysis and conduct independent systems analysis of business processes.
- Ability to maintain and prepare complex, comprehensive, and confidential reports.
- Ability to communicate effectively both verbally and in written communication.
- Ability to lead and perform threat hunting activities including analysis of threat intelligence, detection and evaluation of IOCs, and escalation of incidents.
- Ability to evaluate vendor solutions, make recommendations, and lead projects for deployment and/or enhancement of security systems.
- Ability to understand the NIST cybersecurity framework and application of its controls in operational security.
- Skill in implementing enterprise security best practices including encryption, implicit and explicit permissions, multi-factor authentication, auditing and digital forensics, and data retention.
- Skill in data analysis, problem solving, and critical thinking.
- Ability to take initiative and seek innovative solutions.
- Ability to perform tasks with limited guidance and supervision.
- Ability to cooperate with others by sharing information, presenting ideas and concerns, and answering questions.
- Ability to use sound judgment in recognizing scope of authority.
- Ability to establish and maintain effective working relationships with those contacted in the course of work.

MINIMUM QUALIFICATIONS:

- A bachelor's degree from an accredited college or university in Information Technology or a closely related field.
- Four (4) years of experience working in an IT position.
- An equivalent combination of education and experience may be considered.

PREFERED QUALIFICATIONS:

- Four (4) years' experience in a dedicated cybersecurity role.
- Four (4) years' experience with directory services design and implementation, particularly Microsoft Active Directory, Azure, LDAP, and DNS.
- Possession of an industry security certification (CISSP, CISA, SSCP, CEH, etc.)

ENVIRONMENTAL FACTORS and WORKING CONDITIONS:

- Work is performed in an indoor and outdoor environment.
- Regular and reliable attendance; may work more than forty hours in a workweek without additional compensation to perform assigned job duties, including weekends, evenings, early morning hours, and holidays as required. Must be able to respond to critical cyber incidents outside of normal business hours.

SPECIAL REQUIREMENTS:

- Individual must be deemed acceptable based on Arizona Criminal Justice Information System background check and a screening by the Oro Valley Police Department.