CYBER SECURITY ANALYST

Salary Range: $120,000-$140,000 (Exempt)   Location: El Monte, CA

9/80 Schedule: Monday-Thursday 7:30am- 5:30pm, Every other Friday 7:30am-4:00pm

JOB SUMMARY

The Cyber Security Analyst is responsible for managing and securing the organization's information systems, ensuring compliance with security policies, and protecting sensitive data from cyber threats. The Cyber Security Analyst will play a critical role in implementing security measures, monitoring systems for vulnerabilities, and responding to security incidents.

DUTIES AND ESSENTIAL FUNCTIONS

Performs a variety of tasks and duties including, but are not limited to, the following:

- Administer and manage security tools and technologies, including firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection solutions.
- Monitor and analyze security logs and alerts to detect and respond to potential security incidents.
- Implement and manage identity and access management (IAM) systems, including user provisioning and de-provisioning for Office 365 and Azure environments.
- Configure and enforce conditional access policies to ensure secure access to applications and data based on user context and risk levels.
- Implement multi-factor authentication (MFA) to strengthen security for Office 365 and other critical applications.
- Respond to and investigate security incidents, coordinating with IT and other departments to remediate vulnerabilities.
- Maintain incident response plans and participate in post-incident reviews to improve security processes.
- Conduct regular internal and external vulnerability scans to identify security weaknesses and ensure compliance.
- Perform penetration testing and threat assessments to simulate attacks and evaluate the security posture of the organization.
- Develop, implement, and maintain security policies, procedures, and guidelines specific to Office 365, Azure, and other cloud services.
- Ensure compliance with regulatory requirements and industry standards.
- Provide security awareness training to employees to promote a culture of cybersecurity within the organization.
- Develop materials and resources to support ongoing security education.
- Maintain detailed documentation of security configurations, incidents, and response actions.
- Generate regular security reports for management and compliance audits.
- Other tasks and duties as required.

SKILLS, KNOWLEDGE AND PHYSICAL REQUIREMENTS

- Strong knowledge of security technologies, including firewalls, VPNs, IDS/IPS, and antivirus solutions.
- Experience with Office 365 security configurations, including conditional access and MFA.
- Proficiency in Azure security concepts and tools.
- Familiarity with internal and external scanning tools and techniques.
- Knowledge of security frameworks and standards.
- Strong problem-solving and analytical skills.
- Excellent communication and collaboration skills.
- Ability to work independently and manage multiple priorities effectively.

- Ability to perform repetitive physical activities using feet, legs, hands, and arms, and which include use of keyboard, walk, sit, stand, bend, stoop, climb stairs, lift up to 35 lbs., reach, grasp, push, and pull.

EDUCATION, TRAINING AND EXPERIENCE

The following are required:

- Bachelor's degree in Cyber Security, Information Technology, or a related field.
- 4-6 years of experience in cyber security, IT administration, or a related role.
- Relevant certifications such as CompTIA Security+, Certified Information Systems Security Professional
- (CISSP), or Certified Ethical Hacker (CEH) preferred.
- Valid California Driver's License and acceptable driving record.

To apply, submit a detailed resume to HR@sgvwater.com with "Cyber Security Analyst" in the subject line