Information Security Analyst

Definition:

Under the direction of the Kern County Deputy Chief Information Technology Officer, or designee, performs the day-to-day operations of the in-place security solutions and works with other Security Team personnel in the identification, investigation, and resolution of security issues and incidents detected by those systems.

Duties may include, but are not limited to, the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines, and procedures as well as conducting vulnerability audits and assessments. The Information Security Analyst is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures, and guidelines and to actively work towards upholding those goals.

Essential Functions:

- Monitor all in-place security solutions for efficient and appropriate operations.
- Review logs and reports of all in-place devices, whether they be under direct control (i.e. security tools) or not (e.g. workstations, servers, network devices). Interpret the implications of that activity and devise plans for appropriate resolution.
- Participate in investigations into problematic activity.
- Participate in the design and execution of vulnerability assessments, penetration tests, and security audits.
- Assist in incident response efforts and the remediation of threats and vulnerabilities.
- Provide on-call support for end users for all in-place security solutions.
- Assist asset owners, maintainers, and supporters in securely configuring their systems and applications using established security best practices and County policy.
- Assist in the deployment, integration, and initial configuration of new security solutions and of any enhancements to existing security solutions.
- Maintain up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes, and the development of new attacks and threat vectors.
- Participate in the planning and design of enterprise security architecture.
- Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures).
- Participate in the planning and design of an enterprise business continuity plan and disaster recovery plan.
- Performs other job-related duties as required.

Employment Standards:

A bachelor's degree from an accredited college or university, in computer science or information technology related field AND two (2) years of experience in desktop or network management and administration for a department or organization.

OR

An associate degree or sixty (60) semester or ninety (90) quarter units from an accredited college or university, in computer science or information technology related field AND four (4) years of experience in desktop or network management and administration for a department or organization.

OR

Completion of an accredited trade or vocational school training program in computer repair, computer science or information systems; AND four (4) years of experience in desktop or network management and administration for a department or organization.

OR

Six (6) years of experience in desktop or network management and administration for a department or organization.

Qualifying experience must have been within the last seven (7) years.

A valid Class “C” California Driver's License is required at the time of appointment.

Knowledge of: antivirus and end point management practices and techniques; working technical knowledge of the Microsoft Defender suite; strong understanding of IP, TCP/IP, and other network protocols; strong understanding of Windows Desktop and Server operating systems; familiarity with Microsoft Sentinel, Tanium, PRTG, and other monitoring systems.

Ability to: conduct windows server administration; understand and utilize Microsoft Azure cloud environments; work with PowerShell and other scripting languages.

A background check may be conducted for this classification.

All Kern County employees are designated "Disaster Service Workers" through state and local laws (CA Government Code Sec.3100-3109 and Ordinance Code Title 2-Administration, Ch. 2.66 Emergency Services). As Disaster Service Workers, all County employees are expected to remain at work, or to report for work as soon as practicable, following a significant emergency or disaster.

New Job Specification
May 2023
Item No. 2389