6635 S. Dayton Street, Suite 130
Greenwood Village, CO 80111

www.lsquarellc.com | 303-495-5908

Splunk SME (ISIRA) Location: Carlsbad, CA

Location: Carlsbad, CA

- Position Requirements:
  - Provide expert incident response and analysis and manage security incidents and security response processes relating to deployed Splunk Environment and other security tools including vulnerability management technologies, cloud-based security monitoring capabilities, privileged access management solutions, and data loss prevention technologies.
  - Function as the Security Incident Response Subject Matter Expert (SME) and will interact directly with the IT personnel and management.
  - Provide in depth review of Splunk environment with overview of SIEM capabilities and best practices to align business with incident response requirements.
  - Identify priority SIEM use cases based on business drivers, threats, and personnel available.
  - Review critical assets, log sources, and preventative security devices in order to review and identify what needs to be protected and potential blind spots.
  - Suggest compensating controls and identify active measures that can be taken for incident response.
  - Perform prioritization review: visibility/compliance vs. prevention/protection
  - Identify any compliance and/or operational objectives that must be addressed
  - Review findings/goal alignment: SIEM success strategies and common failure points to avoid, SIEM correlations, reports, and responses, SIEM essential correlations
  - Review backend storage requirements and data warehousing overview
  - Review high availability and disaster recovery, operationalizing SIEM and measuring results (time-based security)
  - Defining SLAs and Record of Authority (ROA)

To apply, submit your resume and cover letter to L2_info@lsquarellc.com