PERFORMANCE RECRUITERS, INC.
Permanent Placement & Consulting Services in Information Technology

Security Engineer – Dallas, TX

Client is seeking a Security Engineer to evaluate, design, plan, implement, and document system hardware, software and security controls. Monitors the performance of systems by performing capacity planning and optimizing established systems. Performs troubleshooting and maintenance functions for infrastructure applications, services, systems and technologies.

- Additional duties include: Design, deploy, maintain, and troubleshoot security technologies including, but not limited to, SEIM, File Integrity Monitoring, IPS, Application/Network Vulnerability Assessment tools, event and log analysis, DLP, anti-virus, anti-malware, and content filtering security systems and devices.
- Review processes, policies and architecture and provide risk-analysis and recommendations to remediate or lower identified risks.
- Ensure business and development teams integrate security into application and product designs, where possible, without adversely affecting the business.
- Research and design secure solutions to technical and business problems that will enhance security posture without adversely affecting the business.
- Develop custom scripts/programs to provide security information and to integrate security tools with existing Freeman security monitoring infrastructure.
- Use security tools to audit, detect and coordinate remediation of any security or infrastructure related issues.
- Provide support to one or more projects simultaneously.
- Research, recommend, and implement streamlined automation processes.
- Ensure that data architectures meet regulatory and legal compliance.
- Provide in-depth support for information security incidents including, but not limited to, internal violations, hacker attacks, virus, and system outages.
- Evaluate and recommend security controls, which includes routinely assessing their effectiveness in limiting security risks to the organization
- Participate in periodic information systems risk assessments.
- Recommend and evaluate security tools to identify more efficient and effective security measures.

Requirements:

- Knowledge of information security principles and best practices
- Knowledge of PCI compliance standards
- Minimum five (5) + yrs experience with stateful firewalls, VPN, remote access methodologies
- Minimum three (3) + yrs experience with regular expressions
- Minimum three (3) + yrs experience performing access control reviews and remediation as it relates to PCI
- Minimum five (5) + yrs advanced network design experience in a multisite environment
- Minimum five (5) + yrs experience with at least two IP packet analysis, vulnerability and network troubleshooting tools: wireshark, tcpdump, nessus
- Must posess advanced knowledge of TCP/IP networking principles
- Experience with at least three of the following solutions, technologies and processes:
- Vulnerability management
- Risk management
- IPS technologies
- Network/application vulnerability scanning Tools
- Web Proxy
- Email content filtering
- Endpoint security tools
- SIEM technologies
- File Integrity Monitoring
- Experience working in, and providing information for, PCI and related regulatory standards environment.

817-329-6830 Tel • 817-329-6833 Fax • PO Box 93538 • Southlake, TX • 76092

rr@prdfw.com • www.prdfw.com

- Knowledge of system hardening, security and access control principals, methodologies and techniques
- Must possess excellent written, verbal, communication and time management skills