



*Permanent Placement & Consulting Services in Information Technology*

## IT Security Architects/Engineers

← Available Jobs

### **Senior Cybersecurity Engineer – Arlington, TX**

**Job Ref: 20181009**

The Senior Cybersecurity Engineer is responsible for developing, deploying, monitoring, tuning, evaluating, reporting and maintaining systems and procedures; to identify and mitigate threats to the corporate network, corporate assets, and corporate users. This team member will identify core requirements, design and implement security technologies, and work with stakeholders to perform ongoing tuning and alerting on those technologies. Said technologies may include but are not limited to: Data Loss Prevention (DLP), Security Incident Event Management (SIEM), User Behavior Analytics, Host Intrusion Prevention (HIPS), and Web/Email Gateway. This team member will be responsible for both technical implementation of systems and communication of security requirements to management and security leadership.

#### **Responsibilities:**

- Engineer, design, install, and support security technologies such as Data Loss Prevention (DLP), Host Intrusion Prevention (HIPS), Security Incident and Event Managers (SIEM), Endpoint Security, Vulnerability Management (VM), Email Gateways, Breach Mitigation, Certificate Management, SSL encryption and decryption, Identity Management, Cloud Security, Database Security, Web Gateways.
- Develop API integration between toolsets to share and correlate data.
- Mature threat intelligence utilization, integrating security solutions to allow retrospective analysis and proactive consumption.
- Proactively identifies potential technologies to better security enterprise information assets.
- Using information from threat intelligence feeds, incident response, and SIEM analysis, identifies and deploys custom rules and policies to security technologies to further protect information assets.
- Works with cybersecurity management to develop and implement project plans to rapidly mature security initiatives.
- Prepare and update information procedures, standards, and/or other technical requirement documents.
- Participate in periodic information systems risk assessments.
- Develop detailed proposals and plans for new information security systems that would enhance or enable new capabilities for network or host systems.
- Recommends and evaluates security tools to identify more efficient and effective security measures.

#### **Qualifications:**

- Strong technical skills and hands on experience in information security as it relates to server security, client security, user security, network communications, and data storage.

**817-329-6830 Tel • 817-329-6833 Fax • PO Box 93538 • Southlake, TX • 76092  
rr@prdfw.com • www.prdfw.com**



*Permanent Placement & Consulting Services in Information Technology*

- Practical experience implementing security solutions, specifically Data Loss Prevention, and performing initial tuning and scanning for confidential data in the environment.
- Proven expertise developing custom rulesets for Data Loss Prevention (DLP) tools to identify specific data types based on feedback and requirements from business stakeholders including Compliance and Legal Counsel.
- Practical experiences scaling DLP solutions to meet enterprise data sizes and performing tuning to manage the amount of alerting that occurs.
- Strong knowledge of core Information Technology concepts such as TCP/IP networking, Windows & Active Directory, Unix/Linux, Mainframe, Cloud Service Providers, Relational Databases, Data Warehouses, and filesystems.
- Strong knowledge of IT technologies and methods to secure them, specifically for databases, SharePoint, storage area networking, cloud-based storage, and data warehouses.
- Practical experience with data loss, data privacy, regulatory requirements.
- Strong knowledge of the OSI model and security that is associated with each layer.
- Experience in setting appropriate priorities for tasks to be accomplished based on project plans and management priorities are required.
- Proven ability to communicate across multiple levels of stakeholders.
- Ability to interpret and document business and technical requirements.
- Good interpersonal, verbal and written communication skills.
- Detail oriented with good time and analytical skills.
- Ability to exercise prudent judgment and offer knowledgeable advice.
- Ability to work both independently and in a team environment.
- Ability to manage multiple projects and tasks.
- Ability to manage production sensitive situations
- Be a reputable representative of the department
- 3 to 8 years in data loss prevention, cybersecurity, or network operations in an enterprise environment preferred.
- Hands on experience supporting security requirements of a large, global enterprise environment.
- Bachelor's degree in Information Technology (or related field) or equivalent experience is preferred.
- One or more security related certifications, such as CISSP, CCNP-Security, GIAC, CEH, CPTS, is highly preferred.

***Submit your resume for this job by contacting us today!***

[Contact Us](#)