PG&E Talent Connect

Job Posting Title

Cybersecurity Technology Architect, Prn

Job Posting Date: 02/12/2017

Requisition #: 53995971-E01

Job Category: Information Technology

Job Level: 4. Manager/Principal

Company

Based in San Francisco, Pacific Gas and Electric Company, a subsidiary of PG&E Corporation (NYSE:PCG), is one of the largest combined natural gas and electric utilities in the United States. And we deliver some of the nation’s cleanest energy to our customers in Northern and Central California. For PG&E, “Together, Building a Better California” is not just a slogan. It’s the very core of our mission and the scale by which we measure our success. We know that the nearly 16 million people who do business with our company count on our more than 24,000 employees for far more than the delivery of utility services. They, along with every citizen of the state we call home, also expect PG&E to help improve their quality of life, the economic vitality of their communities, and the prospect for a better future fueled by clean, safe, reliable and affordable energy.

Pacific Gas and Electric Company is an Affirmative Action and Equal Employment Opportunity employer that actively pursues and hires a diverse workforce. All qualified applicants will receive consideration for employment without regard to race, color, national origin, ancestry, sex, age, religion, physical or mental disability status, medical condition, protected veteran status, marital status, pregnancy, sexual orientation, gender, gender identity, gender expression, genetic information or any other factor that is not related to the job.

Department Overview

The Cybersecurity team enables PG&E to achieve its mission by providing governance, oversight, and support of operational resiliency and asset safeguards in a relevant, timely and data-driven manner. The team consists of security professionals, each with multiple years of experience in their chosen discipline:

- Cybersecurity Risk & Strategy
- Cybersecurity Project Management
- Policy, Compliance Management, Training, & Awareness
- Risk Monitoring & Incident Management
- Control Assessment & Verification
- Business Planning & Control

Working together, we review the current cyber threat landscape and lend our expertise to help the company understand it’s security posture and act on the highest priority risks.

The Cybersecurity team takes a proactive approach to security by focusing on the cyber risks PG&E faces. Cybersecurity's methodology and framework synthesizes current legal, regulatory, and operating mandates with PG&E’s business goals and operations. By taking this information and focusing on the cyber risks unique to individual Lines of Business (LOB), Cybersecurity helps PG&E’s LOBs make informed decisions about where to invest their resources.

Position Summary

The Cybersecurity Technical Architect, Principal, serves as a technical interface and subject matter expert to design, develop, and implement technical solutions that fulfill risk management strategies, to ensure the maintenance of the cybersecurity posture of production systems and the safe delivery of all new technologies across the lines of business.

We are hiring for multiple positions in the following Line of Business specialty areas:

Customer Care, Human Resources, External Affairs and Public Policy, and Regulatory Affairs.
• Understanding of one or several of the following items is highly preferred: Network Security; Identity and Access Management; System Security, Data/Database Security, Cloud Security, Internal/External Web Security, Remote Access Security, Mobile Technologies Security

Electric Transmission and Distribution, Generation, and Energy Policy/Procurement.
• Understanding of one or several of the following items is highly preferred: Industrial Control Systems:
EMS, EDMS, RAS, SCADA, Fault Locations, Outage Management Systems, Distributed Controls, Trading Systems, Data Request Systems, GIS, NERC CIP Standards and Requirements, Modbus, NDP, TCP, IP, IEC 61850, Networking Technologies, Mobile Technologies

Information Technology, Finance & Risk, and Enterprise Programs.
• Understanding of one or several of the following items is highly preferred: Network Security: Firewalls, Segmentation, Protocols, Identity and Access Management, System security, Data Security, Cloud Security, Database Security, Internal/External Web Security, Remote Access Security, Mobile Technologies Security, Accounting Systems

The headquarters and preferred location is San Francisco, CA, however, depending on the specialty area, alternate work locations of San Ramon or Sacramento, CA, may be considered.

Qualifications

Minimum Requirements:
• Bachelor's degree in Computer Science, Information Systems or other related field, or equivalent work experience
• 8 years of related work experience (i.e. Experience in critical infrastructure industry, Information Technology (IT) architecture, Information Technology (IT) security, multi-platform, security technology infrastructure implementation)
• Ability to travel up to 10% to support business needs

Desired:
- M.S. or M.B.A. degree in business administration, computer science, or equivalent preferred
- At least one relevant certification such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), or equivalent
- Utility industry experience
- Experience in critical infrastructure industry
- Expertise in data-protection mechanisms including an in understanding of cryptographic algorithms such as AES, 3DES, RSA, ECC, SHA etc.
- Expertise in data-protection software and hardware solutions including Application, Database, and File level encryption and tokenization solutions
- Native database protection solutions
- Segregation of duties implementations for databases
- Experience in data retention policies
- Experience in data exfiltration techniques and detection and response tools and strategies

- Demonstrated knowledge of:

Technological trends and developments in cyber/information security.
The IT security and threat environment.
Hardware, software, networks and facilities that make up infrastructure.
IT security products and technology
Systems/software development, engineering, integration, testing and evaluation
Cyber/information security management policies, procedures, regulations and governance processes

- Process and systems analysis, testing, application development, network design
- Knowledge of regulatory requirements and utility technologies
- Knowledge of risk management techniques
- Demonstrated problem analysis and decision-making skills
- Ability to communicate and convey complex IT/OT technical security related concepts to business and technology teams.
- Ability to influence and work with and across all levels within the business
- Excellent written and verbal communication skills required
- Anticipates issues and develops innovative solutions
- Management and planning skills
- Ability to successfully manage change
- Ability to foster a work environment in which individuals collaborate in pursuit of a common mission and mutual goals

Responsibilities

- Leads the development and improvement of architectural and security designs for PG&E systems.
- Explores and integrates new cybersecurity testing tools, processes, and capabilities.
- Serves as a subject matter expert to executive leadership on a range of cybersecurity best practices, architectures, solutions and technologies.
- Provides cybersecurity architecture services across specific lines of business to ensure the secure delivery of all technology.
- Supports the development and implementation of cybersecurity strategies across the LOBs.

- Ensures architectures, technologies and solutions align with and integrate regulatory requirements (e.g. HIPAA, SOX, NERC CIP, NRC Title 10, FCC, CPUC) and industry best practices (e.g. ITL, COBIT).
- Provides strategic and tactical cybersecurity guidance for technology (informational and operational) projects, including the evaluation and recommendation of technical controls.
- Develops technical roadmaps and business cases for technology investment.
- Defines cybersecurity protection/defense schemes.
- Provides functional domain expertise to support the definition and implementation of risk mitigation strategies for exposed production systems.
- Designs and implements cybersecurity reference architectures and solutions that are aligned to stakeholder needs and requirements.
- Effectively leverages industry trends and new technologies in order to develop cybersecurity strategies that enhance business value and address business needs.
- Maintains awareness of emerging threats and translates that awareness into architectures and designs that protect critical systems.
- Influences technological and architectural decisions with peer groups.
- Ensures that architectural deliverables (e.g. system lifecycle support plans, concept of operations, operational procedures and maintenance training materials) are properly documented and updated as necessary.
- Provides peer review and support for organizational deliverables.
- Works with senior management to support strategic planning and decision making.
- Coaches and mentors less experienced employees.

Employment Type: Management

Schedule: Full-time

Work Location: GENERAL OFFICE COMPLEX - 77 BEALE ST

City: San Francisco

Zip Code: 94105