Principal IT Security Engineer

The New York City Housing Authority is seeking a strategic and tactical expert as well as a self-directed program leader to serve as Principal IT Security Engineer. Reporting to the Chief Security Officer, the selected candidate is responsible for close partnering with our technology teams; working to continuously strengthen our layered IT Security posture via technical controls, optimized architecture and adherence to leading infosec standards. In this role, the selected candidate will also identify opportunities and drive solutions to completion; assess existing technologies and required control strength with strong emphasis on IT network and host surveillance capabilities.

1. Lead and participate in efforts to engineer complex IT security solutions and coordinate with all necessary subject matter experts. Drive vulnerability mitigation to completion in a matrixed environment gaining concurrence from our technology partners.
2. Train and mentor technology teams and provide guidance for security operations.
3. Analyze risk assessment, intrusion detection, network access control, data loss prevention; perform threat and vulnerability management; identify and access management and encryptions (at rest/motion).
4. Control, assess and design security-related appliances, systems and applications, TCP/IP routing / TLS, routers/switches, VM/Ware, OVM, VPN, BES server, Webfiltering, network surveillance, firewalls, LDAP/A/D authentication, anti-virus, and Windows/UNIX operating systems.
5. Identify security violation causes and potential threats; research and recommend preventive measures.

QUALIFICATION REQUIREMENTS:

1. A baccalaureate degree from an accredited college, including or supplemented by 24 semester credits in computer science or a related computer field and two years of satisfactory full-time computer software experience in computer systems development and analysis, applications programming, database administration, systems programming, data communication, including one year in a project leader capacity or as a major contributor on a complex project; or
2. A four year high school diploma or its educational equivalent and six years of satisfactory full-time computer software experience as described in "1" above, including one year in a project leader capacity or as a major contributor on a complex project; or
3. Education and/or experience equivalent to "1"or"2" above. College education may be substituted for up to two years of the required experience in "2" above on the basis that 60 semester credits from an accredited college is equated to one year of experience. A masters degree in computer science or a related computer field may be substituted for one year of required experience in "1" or "2" above. However, all candidates must have at least a four-year high school diploma or its educational equivalent and at least one year of satisfactory full-time experience in a project leader capacity or as a major contributor on a complex project.

Special Note:
To be eligible for placement in Assignment Level IV, in addition to the Qualification Requirements stated above, individuals must have one year of satisfactory experience in a project leader capacity or as a major contributor on a complex project in data administration, database management systems, operating systems, data communication systems, capacity planning, and/or on-line application programming.

EXPERIENCE PREFERRED:

1. Ten plus years of progressive experience in IT security/network management; operational and security experience in large network, wintel, and UNIX server environments.
2. Experience in key related technologies such as firewalls, routing, DNS, LDAP, MS Exchange and VPN.
3. Prior demonstrated ability to assess systems, networks, applications, and databases for security vulnerabilities; infrastructure capabilities and design mitigating controls.

4. Understanding of industry best practices, for systems security engineering is desired but not essential i.e. ISO 27001 and NIST 800-53.
5. Commitment to continued learning in the field of IT Security Engineering, Risk Assessment and or Risk Management
6. Possession of at least one operational and one security certification in the following (or related) CCNP, CCSP, MCTS, MCSE, CEH, CISM, CISSP is required.
7. Significant hands-on technical experience a must.

SKILLS DESIRED:

1. Strong understanding of enterprise-level technology solutions.
2. Ability to work in a fast paced, changing environment; to quickly learn key security technologies and approaches.
3. Able to communicate risk and security issues in business context (i.e., translate technical risks to business risks)
4. Strong planning and organizational skills.
5. Strong team work, collaboration and leadership skills.
6. Excellent verbal, written, communication and interpersonal skills.