**Description**

SAIC has an opening for a Senior Cyber Security Engineer to join our talented, dynamic team. The key responsibilities for this position include:

+ The Senior Cyber Security Engineer requires information technology experience in the methods, procedures and actions required to protect and secure information system hardware and software against malicious and damaging attacks and actions.

+ Responsible for cyber security tools and network topologies.

+ Understanding of Application Penetration and Intrusion Testing software and methods of deployment.

+ Maintain environment in a safe and secure system based on sound design and implementation techniques.

**Required Skills:**

+ Able to utilize cyber security industry standard methods in providing secure systems

+ Knowledge of Nessus

+ Knowledge and experience in Cyber Security Tools, Network topologies

+ Knowledge of implementation and security levels and roles necessary for successful deployment.

+ Will be required to scan, monitor and report on system vulnerabilities

+ Will work in close contact with the Information Security Office in surveillance of user, software and network assets for appropriate use and enterprise wide protection

+ Must Stay abreast of current cyber security trends relevant to the clientâ€™s business and system security Â·

+ Working knowledge in NIST RMF framework and Authorization to Operate (ATO) process

+ Understanding of NIST SP 800-53 Rev 4 Controls

+ Hands-on experience with GRC tools â€“ for example, eMASS

+ Experience in information security controls self-assessment,SCA and external and third-party assessments and audits

+ Foster an innovative and inclusive team-oriented work environment

+ Demonstrate technical capabilities and professional knowledge

+ Must be well versed in Cyber Security Tools, network topologies, intrusion detection,PKI, and secured networks.

+ Must have familiarity and experience in the implementation of cyber security regulations

**Qualifications**

**Required Qualifications and Skills:**

+ Bachelorâ€™s degree in Computer Science, Information Systems/Technology or engineering discipline preferred Â·

+ At least 10 years relevant experience required or 14 years required in lieu of degree

+ 10 years of relevant experience may be substituted for education Preferred Experience Strong verbal and written communication skills.

+ Attention to detail and excellent customer service.

+ Ability to work well in a team environment.

+ Capable to work under pressure, handle multiple tasks simultaneously.

+ OSCP Certification Familiarity with VA 6500 and NIST 800-53 VA or DOD Experience Industry certifications highly desired, such as OSCP and CISSP

+ IT experience with Cyber Security Policy and threat mitigation.

+ Must be well versed in Cyber Security Tools, network topologies, intrusion detection,PKI, and secured networks.

+ Must have familiarity and experience in the implementation of cyber security regulations

Target salary range: $100,001 â€“ $125,000. The estimate displayed represents the typical salary range for this position based on experience and other factors.

Covid Policy: SAIC does not require COVID-19 vaccinations or boosters. Customer site vaccination requirements must be followed when work is performed at a customer site.
REQNUMBER: 2205428-US-United_States