Cyber Security Engineer

3710 Rawlins St, STE 1420
hr@neucore.io
Phone :
Web : neucore.io

Job Summary

Vacancy : 1
Deadline : Jan 01, 1970
Published : Mar 24, 2023
Employment Status : Full Time
Experience : Any
Salary :
Gender : Any
Career Level : Mid Level
Qualification : Bachelors

Job Description

The Cyber Security Engineer is responsible for ensuring the organization's computer systems and networks are secure and protected from cyber-attacks. They will be responsible for implementing and maintaining security protocols, conducting vulnerability assessments, and responding to security incidents. The Cyber Security Engineer will also work closely with the IT team, vendors, and other stakeholders to identify and mitigate security risks and ensure compliance with industry standards and regulations.

Education & Experience

Implement and maintain security protocols and technologies, including firewalls, intrusion detection systems, and antivirus software. Conduct vulnerability assessments and penetration testing, and identify security risks and vulnerabilities. Monitor network and system logs, and respond to security incidents in a timely manner. Develop and maintain security policies and procedures, and ensure compliance with industry standards and regulations. Collaborate with IT team members, vendors, and other stakeholders to implement and maintain security solutions. Provide technical guidance and support to IT team members and stakeholders, and ensure successful knowledge transfer. Conduct security awareness training for end-users, and promote a culture of security awareness. Participate in security audits and compliance assessments, and address any findings and recommendations.

Must Have

Bachelor's degree in Computer Science, Information Technology, or a related field. Minimum of 3 years of experience in cyber security engineering, with experience managing complex security infrastructures. Strong understanding of cyber security threats and vulnerabilities, and knowledge of security protocols and technologies, including firewalls, intrusion detection systems, and antivirus software. Experience with vulnerability assessment and penetration testing tools, such as Metasploit, Nmap, and Nessus. Knowledge of security standards and regulations, such as HIPAA, PCI-DSS, and GDPR. Strong analytical and problem-solving skills, with the ability to identify and mitigate security risks and vulnerabilities. Excellent communication and interpersonal skills, with the ability to work collaboratively with other IT team members and stakeholders. Industry certifications such as CISSP, CISM, or Security+ are preferred.

Educational Requirements

Bachelors

Compensation & Other Benefits

As per company policy