https://reliablestaffing.com/job/security-engineer-iii-lab-full-time-rscny4405/

Security Engineer III – Lab-Full Time-RSCNY4405

Description

General Responsibilities:

Security Engineer III will be responsible to plan, design, implement and support various security technologies that are used to protect the Mediacom network from external and internal threats. The Security Engineer III is a technical, hands-on expert that is responsible to protect confidentiality, integrity, and availability of networks, systems, and data based on the security policies, standards, compliance regulations, and industry best practices.

Key Responsibilities are –

• Work closely with various internal and external business units to communicate security concepts, define security requirements, controls, vulnerabilities, etc., and maintain a strong working relationship

• Assist with short-term and long-term security strategies that are aligned with Mediacom's business objectives while working with other team members on tactical projects.

• Evolve and maintain overall security architecture

• Participate and contribute to different industry-related security forums

Specific Responsibilities:

• Administer/lead network and application security efforts for a large enterprise and service provider network

• Audit, optimize, and maintain network security infrastructure including firewalls, VPN, intrusion detection/prevention, Network, and Endpoint Detection and Response platforms (NDR/EDR), netflow based tools, URL filtering, NAC, etc.

• Assist in evaluating and developing solutions for complex network security and protection technologies for enterprise and service provider environment including but not limited to Advanced Breach Detection/Mitigation, DDoS attack detection/mitigation, etc.

• Manage and administer Security Incident and Event Management (SIEM) tools, network and system forensics tools

• Analyze network traffic flow between multiple hosts spanning firewalls in different geographical locations to protect appropriately

• Assist with periodic threat and vulnerability assessment, penetration testing, and web application assessments to identify security risks across the company

• Work with an internal and external audit to ensure compliance to appropriate regulations and data protection directives (PCI, CPNI, CCPA/CPRA and CALEA, etc.)

• Initiate and manage special projects related to information security that may be needed to appropriately respond to ad-hoc or unexpected information security events

• Assist in developing security policies, standards, guidelines, procedures

Industry

Engineering

Qualifications

Preferred Experience / Skills:

• Bachelor's degree in Computer Science, Telecommunications or Information Technology is required

• 5+ years technical hands-on security experience

• Extensive experience with firewall technologies, IPS/IDS, VPN, SIEM, netflow, NAC, vulnerability scanning tools, URL filtering, DLP, EDR, AppSec DAST/SAST platforms and other security tools

• Working knowledge and experience with Cybersecurity and Risk Management frameworks such as COBIT, NIST CSF, and ISO 27001 is a plus"

"• Strong analytical and problem-solving skills, with an ability to assimilate, analyze and correlate large amounts of forensic data from the various networks, operating systems, application, and security devices, logs, and alerts

• Experience in security incident handling, operations, and forensics

• Experience in security assessments, penetration testing, and web application assessments preferred

• Experience in handling security for a large enterprise network or service provider network preferred

• Strong interpersonal and communication skills

• Ability to work well under pressure, meeting multiple deadlines

• Ability to present and

• Assist in developing a security awareness program
• Perform other duties as requested by supervisor

Job Location
501 Fifth Avenue, 3rd Floor, 10017, New York, New York, United States

Date posted
March 6, 2024

Base Salary
$ 190,500

Employment Type
Full-time

Hiring organization
Reliable Staffing Corporation

Contacts
RSCNY4405

communicate clearly with technical and non-technical staff as well as senior management
• Ability and willingness to take on additional tasks as assigned
• Security certifications such as CISSP, CISA, CISM, CRISC, OSCP ,and SANS GIAC is a plus”

Button
Button