# Network Security Analyst Job Description

**Duties and Responsibilities:**

- Continually monitor the company's intrusion detection systems
- Create technically detailed reports based on findings of intrusions and events
- Assist in conducting computer incident investigations
- Perform assessment and analysis on anomalous network and system activity
- Responsible for troubleshooting and problem-solving security related client issues
- Required to provide quality customer service to clients
- Proffer recommendations on modifications to access control lists to prevent and mitigate intrusions
- Responsible for the design, implementation, and maintenance of network technology services to ensure confidentiality, integrity, and availability of the company's information assets
- Responsible for the deployment and administration of network access control lists, firewall rule sets, Virtual Private Networks (VPN), Network Access Control (NAC), etc.
- Undertake the administration and maintenance of the department's competence for real-time alerting and digital forensics
- Responsible for the implementation of the unit's vulnerability scanning program
- Collaborate with the IT department to ensure timely implementation of controls, including patching, with minimal impact on the business operations.

## Network Security Analyst Requirements – Skills, Knowledge, and Abilities

- Education: Applicants for the network security analyst job require a Bachelor's degree or initiative and a personal interest in Information Technology Security and equivalent experience
- Knowledge: They must demonstrate strong knowledge of computer security concepts and knowledge of computer programming and scripting languages. Also, previous scripting and coding experience are desired but not necessarily a requirement for securing a network security analyst job
- It is also vital that they are familiar with computer forensic tools FTK, or other network forensic applications
- It is also crucial that they have an advanced understanding of current threats and trends present in the information security and technology field as well as advanced knowledge of network technologies and protocols
- They also require an understanding of network hardware devices and experience configuring Access Control Lists or other firewall or router configuration experience
- Depending on the needs of the recruiter, they may also require knowledge of Linux/UNIX and Windows OS security: network security analysis tools such as Snort, TCPDUMP, Wireshark, and other Host or Network-based Intrusion Detection Systems; and experience with system vulnerability assessment
- Certifications: They must have the ability to quickly obtain and maintain active security certifications such as CEH, DFR, CySA+, GCIA, GCIH, GICSP, or SCYBER) and IAT II (CCNA, CySA+, GICSP, GSEC, Sec+, or SSCP
- People skills: They require the ability to relate with and influence people from different background
- Communication skills: They require the ability to clearly and effectively convey both technical and non-technical information to clients
- Flexibility: They must be able and willing to work rotating shifts when necessary.