



PROFESSIONAL SUMMARY

Experienced Network Security Administrator with over 8 years of hands-on experience in safeguarding network infrastructures for major organizations. Expert in deploying robust security measures, managing firewalls and VPNs, and conducting vulnerability assessments to protect sensitive data and ensure compliance. Adept at identifying and mitigating security threats and optimizing network resilience.

EDUCATION

2014 - 2016

Bachelor of Science in Computer Science

University of Alabama / United States, Montgomery, AL

Technical Proficiencies

- **Security Tools:** Snort, Wireshark, Nessus
- **Operating Systems:** Windows Server, Linux
- **Network Protocols:** TCP/IP, UDP, HTTP/HTTPS, DNS
- **Security Standards:** ISO/IEC 27001, NIST Cybersecurity Framework

SKILLS

- Network Security Design Expert
- Intrusion Detection & Prevention Systems (IDS/IPS) Expert
- VPN Configuration Expert
- Security Information Expert
- Risk Assessment Expert
- Network Protocols & Encryption Expert
- Regulatory Compliance (GDPR, HIPAA, PCI-DSS) Expert

EXPERIENCE

2019 - Now

Senior Network Security Administrator AT&T / United States, Montgomery, AL

- Monitor network traffic and security alerts, promptly addressing potential threats and reducing incident response time by 30%.
- Conduct regular vulnerability assessments and penetration tests to identify and address security weaknesses.
- Develop and enforce security policies and procedures, providing training to staff on best practices and incident response protocols.
- Collaborate with IT teams to integrate advanced security measures into existing infrastructure, improving overall network performance.

2016 - 2018

Network Security Analyst Bank of America / United States, Montgomery, AL

- Managed and configured firewalls, VPNs, and antivirus solutions to protect against a variety of cyber threats.
- Monitored network activity and logs to detect and respond to potential security incidents, significantly minimizing security breaches.
- Assisted in developing disaster recovery plans and conducted drills to ensure organizational preparedness.
- Analyzed system vulnerabilities, providing detailed reports and recommendations to senior management.