

IT Security Analyst Sr IT Security Analyst Sr Security Engineering - IT Security Analyst Sr  
Greenville, SC Authorized to work in the US for any employer Work Experience IT Security Analyst  
Sr FIS Global - Greenville, SC July 2018 to Present Implement security solutions that require  
analysis and research for complex projects. Perform risk assessments, firewall management,  
implement best security practices, monitor security advisory boards and mitigate vulnerabilities.  
Technologies used daily include but not limited to SolarWinds, Cisco ASA, Fortinet, FortiAnalyzer,  
HPNA, LogRhythm, RSA SecureID and FireMon. Security Analyst III Windstream - Greenville, SC  
October 2012 to July 2018 Experience with network architecture, network reliability & root cause  
analysis of network and security events. Experience troubleshooting WAN connectivity issues and  
performing configuration changes to Juniper MX960's. Experience with FortiGate 5101C blades  
and Cisco ASA 5500-X series security gateways. Experience with FortiGate enterprise NGFW  
firewalls stationed at customer premise. Experience with FortiManager and FortiAnalyzer to  
monitor FortiGate security gateways, collect logs and generate security reports. Experience  
supporting FortiToken 2FA and FortiClient Endpoint Compliance. Maintain WIFI gateways and  
implement captive portal or 802.1x for AAA purposes. Manage DMZ environments and related  
policies to provide secure posture from corporate network. Implement Arbor Networks DDoS  
security solutions to mitigate attacks and maximize system up time. Implement security best  
practices on security gateways to prevent unauthorized access and exposure to common  
vulnerabilities and exploits. Create access-list to restrict or permit traffic. Manage dynamic  
disaster recovery and fault tolerant and environments. Configuration and troubleshooting of MPLS,  
VRF and L3VPN routing concepts. VPN technology (remote access, site to site, IKE/IPsec  
lifecycle, failover tunnels). Implement SD-WAN solutions to optimize uptime and prioritize business  
critical traffic. Implement defense in depth and system hardening of hardware devices. IDS/IPS  
configuration, maintenance and fine tuning. Implement Data Loss Prevention rules to prevent  
critical data from leaving network. Manage web proxies and application layer gateways to filter  
internet content. Identify and react to network attacks, viruses and intrusions. Review and  
authorize change/patch management procedures. Review system event logs for suspicious

activity and IOC. Work with hardware vendor to address IP and Security events with the purpose of reaching a resolution or identifying an unknown bug. Develop processes, guidelines and procedures for troubleshooting security events and IP services. Create security baseline configurations and standards to ensure consistent layer of network security. Knowledge of NIST security framework. Serve as CSOC subject matter expert and conduct training sessions to maintain security and operational awareness amongst the team.

**Network Analyst Windstream - Greenville, SC April 2006 to October 2012**

Performed Layer 2/3 network support on Cisco 7200/7600 and Juniper MX series routers on ISP backbone. Administered configuration changes to Cisco 2900/3800 series routers at customer premise. Administered configuration changes and troubleshoot issues on Cisco 3800 series Catalyst switches. Troubleshoot complex LAN/WAN topologies including route protocols BGP and EIGRP. Configured and maintained load balanced data gateways across dual WAN environment. Configured and maintained wired and wireless failover topologies. Configured DHCP, NAT, PAT, access list, static, QoS and dynamic routing. Administered configuration changes to VRF and MPLS cloud environments across multi-vendor hardware. Troubleshoot outages affecting single and multi-site enterprise accounts across layer 2/3 technologies. Isolate core IP network outages caused by routing protocol or hardware failure across multi-vendor network infrastructure. Engaged carriers for service repairs to Fiber, T1, DS3 and PRI transports. Monitored and reacted to network events using Netcool, Solarwinds and Naigos. Resolved network impacting events and track resolution within established service level commitments by using appropriate diagnostic procedures, tools and processes.

**Education**

Associates of Computer Technology in Computer Technology Spartanburg Community College

**Skills** Bgp, Cisco, Juniper, Mpls, Switching, Vpn, Ipsec, Nmap, Wireshark, Dns, Encryption, Ftp, Sntp, Snmp, Security Certifications/Licenses

**Fortinet Network Security Architect - NSE 7 August 2019 to August 2021**

The NSE 7 Network Security Architect designation recognizes advanced skills in deploying, administering, and troubleshooting Fortinet security solutions.

**Fortinet Network Security Analyst - NSE 5 August 2019 to August 2021**

The FortiGate Security Management and Analysis NSE 5 designation identifies your ability to use the FortiManager and FortiAnalyzer to

provide Network Analysis and Reporting. CompTIA CySA+ May 2019 to May 2022 CySA+ credentialed holders are recognized as possessing the knowledge and skills required to configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization. CompTIA Security+ CE May 2019 to May 2022 Security+ credential holders are recognized as possessing superior technical skills, broad knowledge and expertise in multiple security-related disciplines such as network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security, access control, identity management and cryptography. Additional Information SKILLS \* Routing and Switching: BGP/ MPLS / VLS / VRF / VPN \* Knowledge of NMAP / SMTP / DNS / NAT / SNMP / Wireshark / Encryption / SSH / FTP / DMZ / IPsec \* Hardware: Juniper / Cisco / Fortinet / Arbor

Name: Allison Jacobs

Email: annapena@example.net

Phone: 001-833-955-2799x633