Security Administrator/ Analyst Security Administrator/Analyst Security Administrator - Samsung SDS Clifton, NJ Authorized to work in the US for any employer Work Experience Security Administrator/ Analyst Samsung SDSA - Ridgefield Park, NJ August 2017 to Present Monitor Arcsight to find and test instances of SQL injection, XSS, Prohibited Method, and Command Injection attacks against internal and external sites. Use Peakflow TMS to report on potential DDOS attacks and prepare mitigation techniques to drop malicious traffic and allow legitimate traffic through the corporate network. Use Burpsuite to test potentially malicious HTTP requests. Monitor QRadar for instances of anomaly traffic on known firewall ports. Monitor RSA Security Analytics for instances of Wannacry ransomware and for malicious software downloads. Use Netshield to block malicious URI and IP addresses from users. Upload unknown instances of malware to AhnLab AMP for analysis and report results. Test potential malicious software through Fire Eye Malware Analysis and Cisco Threatgrid sandbox environments. Remediation Engineer Varonis - New York, NY January 2016 to April 2017 Train customers on best practices to mitigate insider threats and vulnerabilities. Mitigate potential threats through identification of individuals with improper access. Working with unstructured and semi-structured data, including sensitive files containing SSN, credit cards, patents, etc. Analyze customer environment and architect deployment of Varonis IT Security Suite. Partner with Fortune 500 clients on sizing, installation, and data security remediation engagements. Prepare project specifications and customer facing Statements of Work. Repair inconsistent permissions in Access Control Lists (ACLs) and removed unresolved Security Identifiers (SIDs). IT Support Technician at Pfizer / GE Healthcare / Zoetis Compucom Systems - Florham Park, NJ April 2013 to January 2016 Imaged Windows XP and Windows 7 machines for new hires and contractors. Assisted in migrating user data from Windows XP machines to Windows 7. Troubleshooting user hardware and software issues both onsite and remotely. Document and log tickets via ServiceNow. Configuring client iPhone, iPad and Android Devices via Maas360 Mobile Device Management. Earlier Intern positions at TEAM Academy Charter Schools and ImClone Systems. Remote management and troubleshooting hardware and software issues. Set up and configure Macs and PCs onto domain network. Used Symantec

Ghost 11 to create/restore system images for student laptops and desktops. Create/Delete email accounts in Microsoft Exchange Server 2007. Troubleshooting escalated user issues, including those submitted via the internal Helpdesk. Partner with third-party support centers. Education BS in Information Technology New Jersey Institute of Technology Skills Windows Xp (10+ years), Windows 7 (6 years), Windows 10 (2 years), Microsoft Office (10+ years), Virtualization (6 years), Linux (3 years), Information Technology (5 years), Information Security (5 years), Troubleshooting (6 years), Computer Hardware (6 years), Computer Repair (6 years), Technical Support (5 years), security, access Links https://www.linkedin.com/pub/tom-scancarella/3b/312/712/ Certifications/Licenses CompTIA A+ May 2022 CompTIA Network+ May 2022 CompTIA Security+ May 2022 CompTIA Cybersecuirty Analyst+ May 2022 Additional Information Vmware vSphere/Oracle VirtualBox labs and testing environments. OWASP Top 10 Microsoft Office 2007-2016. Mac OSX and some Linux based OSs such as Ubuntu/Debian, CentOS, and Backtrack/Kali. Nessus Vulnerability scanner. Metasploit Framework, Wireshark protocol analyzer, Cain and Abel, John the Ripper and SSL Strip.

Name: Donna White

Email: zwilcox@example.org

Phone: (986)894-0480x7347