

Systems Administrator/Migration Systems Administrator/Migration System Administrator  
Germantown, MD Ambitious and motivated professional, seeking an opportunity in NOC, Cyber Security, and Windows Administration roles that provide a challenging team work oriented environment. US Citizen. Clearable. Authorized to work in the US for any employer Work Experience Systems Administrator/Migration GEICO - Friendship Heights, MD April 2019 to Present  
Execute Upgrade / Migration tasks -Upgrade Windows 7 to Windows 10 Imaging workstations via SCCM Coordinates with Client End User on expectations and availability to schedule Back-ups and restore tasks. Performs troubleshooting and remediation at Central Office and remote locations. Identifies potential issues that could adversely impact End User experience and follow through on action steps. Escalate to Management on issues that impact the entire operation at a given site Installation and configuration of client software. Acquisition Specialist ManTech International Corporation - Herndon, VA January 2019 to April 2019 Lead the acquisitions project that was migrating old devices to new windows 10 devices. This was the first plan action after KGS was bought out by Mantech. We completed the project in record timing with no issues afterwards with any machines updated and configured all devices before sending them to the KGS offices Provisioned and Imaged all devices before sending Walked through step by step to help users with first time login and additional setups Datacenter Technician AWS - Manassas, VA October 2016 to December 2018 Providing internal and external customers with a single point of contact, and handling & initial identification of security incidents/events. Handled escalated alerts from appropriate personnel. Ran various High Priority audits in the datacenter facility on a daily basis. Managed the Interactions between customers/engineers/technicians, vendors/providers leveraging Remedy while managing network operations using various network management tools, utilizing a solid knowledge of network concepts, protocols, and transport technologies. Escalate and communicate customer issues and network related alerts to NOC and Engineering staff, management and administration as defined by policies and escalation procedures. Responded to emergency network outages in accordance with business continuity and disaster recovery plans, assisting other departments as required. Receive and resolve Severity Level 5-1 (1 being the

highest priority) and IT requests via e-mail and internal Remedy ticket system. Worked with Linux on a daily basis with almost every host running CentOS. UNIX computer skills; Basic Scripting. Experience supporting / troubleshooting distributed / client server / virtualized servers and applications in an enterprise environment >100000 servers. Provide support in the identification, documentation, and development of computer and network security countermeasures. Experience supporting MS Windows infrastructure, including any of the following: Active Directory, WINS, DNS, DHCP, TCP/IP, and Group Policy. Monitor servers, operating systems, network configurations, software applications, and hardware. Administer and monitor system availability and performance tools. Deployment of New servers and Racks. Remotely and Physical configurations of Network Switches, Routers, Firewalls, Load-balancers and Hosts/Racks. Partitioned Drives in hosts to clean raid degradation. Reboot servers and network devices utilizing multiple data sources and tools in the diagnosis and assessment of system degradation. Replaced legacy Cisco WDM with Quanta and ADVA network device. Conducts daily inspections of all data center assets and environment. Ran in house commands on Linux to obtain diagnosis of servers/ network devices. Install, configure, troubleshoot, and maintain server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Support the deployment and integration of security tools. Maintains cabinet drawings, cable runs and other data center documentation. System backups, patching and updates with BigFix, RDP, and SSH. Perform aspects of intrusion detection, log and audit management, network and database vulnerability assessment and compliance management, and security configuration. Used Splunk Search & Reporting in conjunction with Splunk Enterprise Security to identify new network vulnerabilities, examined log files, detect Firebird workstations that have been connected outside the network and report any malicious activity to SIOA. Analyzed packet captures from Defense Center (SourceFire) within Wireshark to investigate suspicious activity further. Configure network scans, schedule network scans to run with bandwidth use in mind, and ensure accurate vulnerability assessment results are generated and made available to appropriate personnel. Develop, update, and maintain internal Standard Operating Procedure for all internal assigned functions. Computer and Network Support

Intern NOCSMART - Gaithersburg, MD February 2014 to September 2014 Install, upgrade, repair, configure, optimize, troubleshoot, and perform preventative maintenance on basic personal computer hardware and all Windows and Redhat, Fedora, CentOS Linux operating systems. Maintain and troubleshoot peripheral computer components. Install, configure and support operating systems such as Microsoft Windows XP/7 and Office suite. Setting up Linux CentOS Samba Servers. Managing RedHat Servers Install and manage LAN/WAN network connected devices such as servers and desktops Support laptops and portable computing devices with network and Bluetooth capabilities Identify personal computer security vulnerabilities and applying patches and updates to mitigate risks. Setup, configure and support RAID 0, 1, 5 & 10 arrays for data security/redundancy. Create network shares using mapped drives and support business data sharing. On site assistance to clients for system repairs. Computer Sales Specialist Best Buy - Germantown, MD August 2012 to January 2014 Sold the latest tablet, computing, and cellular devices. Ran Windows 8 and 7 Setup and installation. Used multiple android and apple operating systems including KIT KAT, JELLYBEAN, And ICE CREAM SANDWICH and the iOS. Ran Microsoft office setup and installation. Performed updates on PC and Tablet devices. Great customer service with countless return customers. Was in top ranks in sales in the MD area in the Computers and Tablets department. Configured hardware in laptops and desktops. Installed ram into laptops and desktops. Upgraded hard drives, network cards, and graphics cards. Worked with an online shipping program. Troubleshooting Microsoft office and other programs Education Bachelor's Degree in CyberSecurity University of Maryland 2022 Skills database (2 years), Linux (2 years), security (2 years), Splunk (2 years), vulnerability assessment (2 years), Talent Acquisition, Interview, Taleo, Bilingual, Human Resource Additional Information TECHNICAL SKILLS Key Skills: AWS Security tools, AWS Macie, AWS Guard Duty, AWS testing, Incident Response, Malware Analysis and Prevention, Vulnerability Assessment, Authentication & Access Control, System Monitoring, Network & System Security, Cryptography, Windows / Linux Systems, System Administration. Specifying Power and Cooling requirements and ensuring Hardware Racking/Stacking completed for new equipment, basic configuration and rollout of new or upgraded

hardware. Tools Used: Kali Linux, Metasploit, Nmap, Nessus, Splunk & Splunk ES, Cobalt Strike, Colasoft Packet, WireShark. Incident response database and tools, AWS in house tools Myday, J5 network testing/ resetting and configuring network switches.

### SUMMARY OF QUALIFICATIONS

Expanding knowledge in Kali, RedHat, Fedora, CentOS Linux, and Bash Scripting. Experience working within a data center or network operation center environment. Experience in maintaining and monitoring server systems. Experience in operating Linux operating systems. Ability to collaborate and partner with teams to overcome challenges. Ability to adapt to changes in a dynamic work environment. Respond to customer phone calls and emails in the NOC and record trouble ticket issues. Monitor Network Conditions both in the office environment and the customer network environment. Follow NOC procedures and processes for daily, weekly, and monthly monitoring, data recording, and network management. Experience troubleshooting integrated and interdependent computer systems. Experience maintaining PCs. Ability to prioritize work based on department and production objectives. Service Management, Project Management, and Inventory Management skills. Excellent written and verbal communication skills. English reading, writing and communication skills. Creating and implementing domain policies and groups across Active Directory. Understanding of DNS, DHCP, TCP/IP, LAN, and VPN. Extensive knowledge in supporting PC/Server based hardware and software problems. Perform a Virus Scan and Malware Identification Scan and eliminate threats. Review latest Common Vulnerabilities and Exposures (CVE) advisories as they apply to our technology stack. Detect potential intrusions and compromises through review and analysis of relevant logs and analytic tools. Conduct security incident investigations on servers and networks. Perform reconnaissance and probing using nmap and Zenmap (GUI version). Perform vulnerability assessment scans using Nessus. Configuring group policy objects and Microsoft baseline security analyzer. Perform protocol capture and analysis using Wireshark. Familiarity with programming languages, Python, Java. Install, configure Linux CentOS, RedHat, and standard operating commands. Expanding knowledge in RedHat BASH Shell, and CentOS Linux. Linux Shell Scripting. Check live systems and open ports, perform banner grabbing and OS fingerprinting. Draw network diagrams of

vulnerable hosts. Research new threats, attack vectors, and risk.

Name: Nicole Sparks

Email: [michaeldurham@example.com](mailto:michaeldurham@example.com)

Phone: 286-309-0209x209