Analyst Analyst Analyst - Network Operations Center Germantown, MD Cyber- Security Analyst /Network Administrator with strong skills in monitoring, detecting, analyzing, understanding and recognizing cyber- security threats, vulnerabilities, exploits and intrusion to network/host-based systems. Professional experience as a NOC and SOC Technician providing tier I and II support to clients on site and remotely as needed. Possess 4 years' experience in security, networking and general IT support. Work Experience Analyst Network Operations Center August 2018 to Present Government of the District of Columbia Providing technical support, maintenance and monitoring of highly available and complex District Government enterprise network infrastructure by performing an initial triage of incidents before troubleshooting and escalating incidents; Monitor global network infrastructure using sophisticated monitoring/ analytic tools like Solarwinds, Splunk, HP AppPulse, Cisco Prime Infrastructure, and SiteScope. Troubleshoot network issues (wired and wireless) and provide network/device configurations by remotely accessing devices at multiple locations which include but not are limited to telecommunications circuits, LAN/WAN systems, routers, switches, firewalls, VoIP systems, servers, storage, backup, operating systems and core applications. Respond and complete network access related request from every D.C Government agencies, e.g., network routing change across multiple agencies, VLAN changes in the routing table, provide Static IP addresses for network devices from excluded IP addresses range per agency's network, and a block MAC Addresses request from the Security Operation Center (SOC) for malicious/ rogue devices from the network via the connected switches, routers and wireless controllers. Provide timely response to all incidents, outages and performance alerts. Categorize issues for escalation to appropriate technical teams. Notify customer and third-party service providers of issues, outages and remediation status. Review new network designs and changes to ensure that they meet Operational Acceptance Criteria and are supportable. Update design documentation for internal and customer support. Ensure network availability maintained and network issues are resolved in accordance with OCTO service level agreements. Ensure accuracy of network documentation and making sure persistent problems are diagnosed and resolved. Use Remedy Ticketing system to track, document and update general issues during and after troubleshooting. Work with internal and external technical and service teams to create and/or update knowledge base articles. Collect and review performance reports for various systems, and report trends in hardware and application performance to assist network engineers to predict future issues or outages and ensure changes do not cause business outages or issues. Support after hour and weekend on-call duties for global trading and office support. Provide VPN Admin support to all D.C Government VPN (internal and external) users by accessing the D.C. VPN Administration portals (Pulse Secure, VPN database, Splunk and kiwi) to make configuration changes to users account and troubleshoot root cause of VPN login issues users maybe experiencing. IT Specialist/Systems Administrator Compass Solutions, LLC - Washington, DC January 2017 to August 2018 part-time) Institution of Higher Education Performed hardware installations, resolve networking issues, printer configurations, clean operating system (OS) installation (Windows & Windows Server, Linux & Linux Server, Unix), troubleshooting network issues and problem resolution, replacing disk drives (Ghost Symantec imaging), NIC cards, memory, and video cards, installing new systems and load sets, installing/upgrading various standard software packages. Provided local and remote troubleshooting through diagnostic techniques and using scripts and checklists as guides. Involved in the installation and rollout of new software packages (Geographic Information System (GIS), Microsoft office, anti-virus and anti-malware), upgrades and new desktop hardware. Maintained IT equipment (phones, desktops, laptops, copiers, printers, scanners, projectors and monitors). Involved in the implementation and management of new pfSense and Fortinet FortiGate firewall/VPN for the D.C. campus and three other remote locations. Managed two computer labs and several classrooms on campus. Stay current with system information, changes and updates. Maintained and updated changes to all the IT/computer equipment on campus using an inventory system. Identified and escalated situations requiring urgent attention. Researched solutions to IT issues using available information resources. Through research and request, pursue opportunities for improved efficiency. Independently audited usage, accuracy, and value of deployed projects. Validated that programs are operating on clean, correct and useful data. Reviews, evaluates, designs, implements and maintains internal and external data. Maintained, analyzed, and managed internal reporting measures. IT Cyber Security Specialist/Network Administrator Compass Solutions, LLC - Washington, DC December 2015 to August 2018 Responsible for triage, prioritization, system log analysis, and initial response to cyber- security incidents and event management; Used SIEM tools such as McAfee Enterprise Security Manager, SolarWinds Log & Event Manager and Splunk to monitor and analyze system logs, network traffic, event data and several alerts from multiple applications and devices connected to the network. Escalated system and application security threats, vulnerability, and flaws to the right department after proactively searching through system logs. Used networking (TCP/IP protocols) knowledge and Network-based Instruction Detection/Prevention Systems Tools to scan, monitor, and detect threats, vulnerabilities and exploits in the network traffic. Ability to detect, false-positive and false-negative alerts while monitoring traffics. Used different penetration testing tools (Nessus, Metasploit, Kali Linux, GFI LanGuard, Nikto) on test areas (labs) for regular vulnerability assessments and remediation on how to improve systems/application security and firewall for host and network-based systems. Actively researched recent/current security flaws, threats, vulnerabilities and exploits before working with security, systems and network engineers to improve system security and firewall rules. Monitored, managed and maintained multiple systems, servers, and the network infrastructure hardware. Managed Windows Server 2012 R2 and 2008, VMware ESXi hosts, DHCP server, Active Directory Domain, DNS record management, NTFS file permissions, Print and FTP server. Managed SharePoint Server and administered user accounts with permissions and privileges. Installed, upgraded and manage new Cisco router/firewall and switches for the location. Used specific tools to monitor/manage network traffics and system logs on the network and servers. Configured and managed phone lines, fax and eFax system. Successfully migrated company's accounting software from a local server to the cloud while providing both local and remote support to maintain and troubleshoot any arising issues. Provided local and remote assistance to users logging in and connecting to company's systems, servers, and networks. Data migration and configuring new systems for users. Performed regular systems/servers' software update and cloud backup solution. Monitored system performance, Server load and bandwidth issues. ZOHO database administrator. Worked along with the Project Manager and Subject Matter Resource as a Functional/Technical Analyst to do an assessment of the George Washington University Hospital's telecommunication and network infrastructure project. ATM Support Intern Guaranty Trust Bank June 2014 to June 2015 Financial Institution Monitored the daily activities of three ATM's and ensured they are all working and dispensing cash accurately. Sorted cash for the ATMs, loaded cash in the ATMs, resolved technical issues within the ATMs and escalated major issues to the appropriate personnel. Assisted tellers in attending to the bank's customers, ensured accurate cash deposits, and withdrawals. Enrolled the bank's customers into the Bank Verification Number (BVN), which is a biometric registration mandated by the Central Bank of Nigeria (CBN) for all accounts holders. Developed and maintained a continuous record database to monitor all tellers' daily activities using Microsoft Access & Excel. Monitored, updated and changed the foreign exchange board to match current market trends in currency transactions. Recorded all cash coming into the bank and cash leaving the bank to Central Bank of Nigeria which included mutilated and old naira notes no longer in service. Reported directly to the ATM staff and the Head of Operations. Education Bachelor of Science in Information Technology in D.C University of The Potomac 2018 Associate of Science in Mechanical Engineering Technology in World Education Services The Polytechnic 2013 Associate degree in Ibadan The Polytechnic 2013 Skills Cisco (3 years), DHCP (2 years), DNS (2 years), exchange (1 year), firewall (4 years), FTP (2 years), Linux (4 years), Metasploit (2 years), Nessus (2 years), networking (4 years), printers (1 year), SIEM (2 years), Solarwinds (3 years), Splunk (3 years), TCP (2 years), TCP/IP (2 years), testing (2 years), testing tools (2 years), Unix (1 year), VMware (2 years) Additional Information Great communication skills (both oral, written and active listening). Ability to work effectively in a stressful situation and under pressure. Strong attention to details. Time Management, Decision Making, Teamwork, and Self-motivation. Ability to prioritize, multi-task, and manage multiple tasks in a timely manner. Conflict Resolution, Creativity, Adaptivity, and Leadership. TECHNICAL PROFICIENCIES: Platforms: Windows OS XP, 7, 8, 8.1&10. Mac OS. Linux (Kali Linux, Ubuntu, Red Hat, Fedora, CentOS, Solaris, Linux Mint, Tails, Open SUSE). UNIX. iOS. Android.

Windows Server 2003, 2008 & 2012. Linux Server (Debian, Ubuntu Server, Fedora Server). Networking: Virtual Private Networks (VPNs). TCP/IP. UDP. VoIP. HTTP. HTTPS. SLL. SSH. SMPT. DHCP. DNS. Ethernet. Wi-Fi. FTP. POP3. IMAP. IRC. IPSec. Internet Key Exchange. OpenPGP. PKI. Kerberos. P2P Protocol. TLS. ZRTP. WEP. WPA. WPA2. Tools: SIEM (Splunk, OSSIM, Prelude, ELK, Snort, OSSEC). Packet Sniffer and Network Analyzing Tools (SolarWinds, tcpdump, Windump, Wireshark, tshark, Network Miner, Fiddler, Capsa). GNS3. Hyper-V. VMware. vSphere. ESXi. Penetration Testing Tools (Nmap, Aircrack-ng, OWASP ZAP, Scapy, NetHunter, splmap, SET, Nessus, OpenVAS, Metasploit Framework, Nikto). pfSense firewall. Hardware: Dell PowerEdge, Dell and Lenovo business laptops & desktops, HP & Canon Copiers/Printers, MacBook, Chromebook, Cisco Routers, Cisco Switches (4500 & 6500 series), Cisco Firewall (Firepower Series), Fortinet FortiGate firewalls, Raspberry pie, iPhone, Android, Projectors (ViewSonic, Optoma, Epson).

Name: Michael Miller

Email: bautistavictoria@example.net

Phone: 629.322.2721x4562