Cybersecurity Analyst (Remote) Cybersecurity Analyst (Remote) Cybersecurity Analyst (Remote) - Xerox Corporation Richmond, VA 6+ years of IT support experience with strong experience in Python scripting, Linux, and AWS Solution Architecture. Experienced associate with a demonstrated history of working in the information security industry. Skilled in customer service, Microsoft Word, Microsoft PowerPoint, Leadership, Microsoft Office, and AWS Solution Architecture.

Certified CompTIA A +, CompTIA Sec+, Logical Operations Certified CyberSec First Responder, (CFR) Certified Microsoft Technology Associate (Networking & Security) professional, CompTIA CySA+, System Security Certified Practitioner, Certified Ethical Hacker v9. Experienced in network appliance configuration, Window and Linux migration and systems and vast knowledge of client and server applications, as well as installation and configuration of wireless network security. Experience with Python programming language. Built dictionary, calculator, and camera software with Python programming language. Professional experience developing and implementing new security systems, programs, protocols, and maintenance of existing systems. Strong written and oral communication skills and the ability to communicate technical information to a non-technical audience. In-depth knowledge of data communications and network experience of operating systems and tools. Deep understanding of current threats and trends in Information Security. Work Experience Cybersecurity Analyst (Remote) Xerox Corporation January 2019 to Present Manage vulnerability remediation of 3,500+ devices(printers, computers, and servers). Use Nessus,vulnerability management tool, to scan for vulnerabilities on devices. Use Tenable Security Center to manage vulnerabilities. Use Servicenow to manage incidents and report vulnerabilities. Use McAfee EPO for endpoint management Use Sharepoint for our team document sharing and to collaborate with team across our workspace. Provide analytics and reporting to internal and external customers printers and servers. Also, use RSA Archer GRC to manager risk and compliance. Help in the development of System Security Plan(SSP). Manages and coordinates resolution of security incidents and problems from identification through implementation of remedies and root cause analysis Perform Root Cause Analysis and remediation for identified security vulnerabilities within the Xerox scope of services. Monitor and

manage Xerox remote monitoring and management tools. Also use this tools to roll out patches and configurations update. Monitor and manage Xerox printer firmware and working through change management processes. Use Xerox internal tools to remotely manage printer firmware. Help in the development of System Security Plan(SSP) to be use in various contracts. Support the asset management activities with a focus on asset database accuracy. Analyzes incidents and problems to identify trends and potential problem areas so that actions can be taken to minimize the occurrence of incidents and to improve the processes to drive sustainable operational improvements

Manage and perform asset configuration testing in a small dedicated test lab. Production Support Specialist(Command Center Operations) Capital One September 2018 to December 2018 Work in the Command Operations Center supporting 100K customers by identifying real time incidents, triaging, resolving or excalating in an effort for customers to have a better experience while during business with the company. Monitor Splunk(network and threat intelligent tool) dashbord for anomalies and alert that are against the normal threshold and investigationg those threat. Run advanced Splunk queries to get details of specific threat. Also use visualization, dashboard, and statistical analysis gather from the advanced search queries to troubleshoot problems. Use Zabbix monitoring tool to detect threat related to application, cloud products, and network. Use Datadog as a advanced tool to monitor and get visibility of Cloud related application, on premise servers, and services. Extensively use PagerDuty as a central incident monitoring tool to recevive alert from monitoring tools to timely respond to incident and to create tickets for the various incident. Use New Relic advanced monitoring tool to get real time visibility of software performance and also use the dashboard to see impact related statistics. Monitor DevExchange dashboard for API Gateway "http status errors" and to use triage the incident from the information gather by using Splunk, Qualys or AWS Cloud Watch. Use AWS Cloud Watch to monitor CPU Utilization and Healthy Host of Varionus AWS instances and Clusters. Use Apica to monitor critical backend API and applications and leverage the data gather from Apica to troubleshoot and resolve incident critical to the business. IT Operations Support Amazon.com - Chester, VA February 2018 to October 2018 IT Operations Support Part of a distinguished IT operations team delivering efficient IT services to

over 3,000 employees to provide the best experience to our customers. Monitor Nagios dashboard(network monitoring tool) for network and application related issues. Use Remedy Ticketing system to create and maintain ticket queue to enhance work related task. Maintenance and installation of 1500 wireless access point(WAP) and IP security camera. Extensively working with Amazon Web Services(AWS) to provide technical support in the network. Performing system imaging on all Computers, Kindles, mobile devises and thin Client used my employees. Use System Center Configuration Management (SCCM) to image thin clients, desktops, Laptops and to deploy window. Write Python scripts for troubleshooting and support. Use Window's Bitlocker to encrypt files on hard drive. Use Linux command line to perform various job task and to run routine maintenance on Unix and Linux operating systems. Like clearing Linux print que on print servers, troubleshooting wireless issues and setting up Linux workstations wiping disk using the dd command. Use SSH, VNC viewer, RDP and Putty for remote access to various systems to perform job related functions. Use password tool to perform password reset for employees. Use Active Directory(AD) setup and updates certificates credential on various window systems. Performed Installation, configurations and maintenance routers, firewall, switches and servers in various Intermediate Data Frame(IDF) and Main Data Frame(MDF). Also monitor the temperature of the IDFs and MDF. Use Window's Migration tool (USMT) to perform migration of associates files from one hard drive to the other. IT Support Technician (Contractor) CompuCom Systems, Inc 2018 to February 2018 Maintenance of Cisco switches, servers and backups systems and troubleshooting of network related problems to achieve full functionality. Testing wireless connectivity and footprint and reviewing the SSID list of the network for malicious SSID on Lowe's Home Improvement stores wireless network in North Virginia. Testing of Point-of- Sales devices for hardware or software key loggers. IT Support Analyst Tabernacle of Praise Intl., VA February 2013 to December 2017 Troubleshoot, repair, maintain, install and perform testing activities on various Microsoft and Cisco router, switches, peripherals, and computer network systems to maintain data communication. Ensure server backups and networked user backups are performed on a regular basis. Test and adjust to appropriate standards, maintain and repair technological

equipment (e.g. routers, switches and peripheral devices.) Install well-functioning LAN/WAN and other networks and manage components (servers, IPs etc.). Perform regular upgrades to ensure systems remain updated and keep records of repairs and fixes for future reference. Develop and implement complex Internet and Intranet applications on multiple platforms. Network Security Analyst World Food Program - LR December 2010 to October 2012 As a member of the Network Security Analyst team, monitored the network layer firewall logs. The Network Security Analyst team was also responsible for the revision of logs and alerts generated by Snort (Network Intrusion Detection and Prevention System), perform investigations, and alert IT supervisor on any malicious activities for relevant action. As the Network Security Analyst Team Lead, performed security patches and updates of the operating systems of our network reset associates password and troubleshoot network connectivity issues. Using Wireshark and Microsoft Baseline Security Analyzer as a secondary tool to analyze packet coming into our network was also part of our work. Education Bachelor's in Information Systems University of Richmond January 2016 to August 2018 Master's of Science in Cyber Security John Hopkins University Bachelor of Science in Mathematics in Chemistry Cuttington University Certificate NetCom Learning Computer Training Institute Skills training, Excel, database, Management Links https://www.linkedin.com/in/emmett-blapooh-404028134/ Additional Information TECHNICAL SKILLS Cloud (Amazon Web Services, Azure), Red Hat Enterprise Linux 7, UNIX/Linux, Windows OS, SCCM, State Migration Tool(USTM), User Windows Server, SQL,TCP/IP, OSI model, Cisco routers/switches, Active Directory, Kerberos Ticketing, Information Security, VoIP, SAN, LAN/WAN, DNS, DHCP, Microsoft Office (Word, PowerPoint, SharePoint, Excel, etc.), Firewall, Wireshark, Oracle, Nessus, Nmap, Cyber Security, Python, Palo Alto Network Firewall, Juniper. Malware analysis, computer hardware/software, Data backups, IP, Network Intrusion Detection, Prevention System, AlienVault, OWASP, SEIM, ZAP, Burp Suite, Vega, Metasploit, Nessus, Nexpose, ArcSight, Splunk, WPA2, Snort, Cyber security threat management. COURSES/CERTIFICATIONS(ACTIVE) Logical Operations Certified CyberSecurity First Responder (CFR) Certified AWS Solutions Architect - Associate CompTIA A+ Qualys Certified

Specialist (SIEM System) CompTIA Certified Cybersecurity Analyst (CySA+) Certified Ethical Hacker (CEH V9) Cisco routing and switching course System Security Certified Practitioner (SSCP) CompTIA Security+ Python Security Professional Certified Microsoft Tech. Associate (MTA) Networking Certified Microsoft Tech. Associate (MTA) Security Palo Alto Networks Firewall Course Microsoft Azure Professional Course SharePoint 2016 Power User Certified Amazon Web Service Solutions Architect - Associate Microsoft Certified Professional Certified CompTIA Security Analytics Professional

Name: Carlos Vasquez

Email: spowell@example.org

Phone: 273-328-7791x154