Security Analyst Security Analyst Security Analyst Lawrenceville, GA Information technology experience with over 10 years of providing Client/Server technical support for medium sized private businesses to large Federal agencies. Providing efforts to secure data incoming and outgoing of the network. Experience diagnosing, troubleshooting and resolving client issues in a timely manner. Experience in supporting government policies and operations and providing efficient service. Work Experience Security Analyst ProCare RX April 2019 to July 2019 Daily duties were to monitor behavior changes from the network eg. applications, servers, firewall, IDS, IPS, anti-virus, email servers. Respond to threats and incidents that may occur against the company's network. Administrator of LogRhythm configuring alerts and rules compliance to the environment. Investigation of alerts and performed cross correlations to determine false or positive threats to the environment.. Customized alerts via LogRhythm to increase the safety of the network Monitored/updated/created necessary policies via Symantec Endpoint. Create and modify firewall rules. Customize weekly vulnerability scans and reports using Tenable io. Monitored servers and network performance using the application manager tool Created the Security Awareness Training course. Created an Incident Response Action plan Revised the Security Policy for the agency. Researched and provided insight to management on how to harden their network and make environment more secure. Perform malware reversal and analysis. Provided Phishing test for the end-users to conduct a study of pass to fail ratio for future analysis. Document technical reports detailing computer evidence discovery and steps taken during the retrieval process and the process of eliminating the threat. Systems Administrator Centers for Medicare and Medicaid Services (CMS) November 2011 to October 2018 Played a major role for Microsoft 365 migrations, Win7 to Win 10 migration. Implemented and conducted the migration of iPad and iPhone project for 120 end-users Implemented patching and updates to workstations and virtual systems. Maintained Group/User security policies, security of folders and files and organized the OU. Managed several Domain Controllers. Performed hardware and software installations and provided high-level customer care, training and technical support. SCCM duties included network protection, management of patching, application packaging, OS deployments. Created new

Accounts and provided operational support for new employees. Responsible for updating and resolving operating systems issues and providing timely support to local and out-stationed VPN users. Conducted vulnerability scans on systems to detect if any threats or attacks were present via NESSUS. Initiated SPLUNK to gather data for real time visibility of alerts of a systems data. Managed SecureTrust to protect data and prevent the data from being lost or misused. Configured and maintained WatchGuard firewall to manage the flow of the networks traffic incoming and outgoing. McAfee NSP (network security platform) was in place on the network to ensure the data and nodes are secure. Responsible for tracking government issued equipment and performing routine inventory procedures through the use of ServiceNow. Actively participate in weekly IT Team meetings with CMS Central Office (Baltimore), to coordinate national efforts and obtain a thorough understanding of CMS policy and security procedures, change management processes and data collection, feedback analysis and corrective action. Maintain servers and workstations via VDI. Decommissioning of virtual servers when now longer needed. Supported the PIV Card systems along with security certificates issues. Supported companies SharePoint site and medical service sites. Provided support for the Companies VPN infrastructure. Provided updates for Anti-Virus definitions on a regular basis. Support Cisco AnyConnect software, kept current the health and the status up to date. Manage software deployment through TEMS Update the employees on the Federal Policies and SOP's Work aside the Security Team if there are any issues compromising the integrity of the network. Maintaining and assigning Group Policies in Active Directory. Analyzing the health of systems via Ivanti for present performances and for future improvements. Monitored assets and virtual servers through McAfee ePO Support Training courses primarily security training for the end users. Tested end-users with fraudulent emails to ensure training was compliance with HIPAA. Provided Tier 3 support when helpdesk issues weren't resolved. Participated with the team members and work alone on many projects to meet company's deadline. Conducted meetings with managers and department heads on how to improve the network and physical environment for security purposes. Responsible for 1st Level Executive from 3 different business units 20+ 24/7 support. Supported servers 2008/2012 in physical and virtual environment. Provided On call and rotational support. Computer Systems Analyst, KForce U.S. Environmental Protection Agency (EPA) August 2010 to October 2011 Performed diagnostics and troubleshooting of system issues, documented help desk tickets/resolutions, and maintained equipment inventory lists. Performed hardware and software installations and provided high-level customer care, training, and technical support. Provided technical support to Local, VPN Network and Lab Software Efficiently completed add / move Request for all federal employees. Created new accounts and provided technical support for new employees. Adding and removing domain controllers from the domain, creating child domains and troubleshooting Active Directory replication issues, DC issues, account creations, access to resources, password issues, file system security issues, Group Policy creation. Upgraded on a regular basis where possible Infrastructure applications that needed to be current with security standards. Migrations of Enterprise print servers from Windows 2003 32 bit standard to Windows 2008 R2 64-bit environment. The creation and management of Virtual Machines, DRS, HA, installing VMware tools, creating templates, deploy Virtual Machines from Templates was part of my duties. Provided current patching and licensing for applications with the SOP of the EPA. Administered the Symantec Endpoint console keeping current of anti-virus definitions, health of systems, leases on licensed software, viewed the companies security status. Tier III Help Desk Support, Perot Systems Centers for Disease and Control and Prevention (CDC) March 2009 to June 2010 3/2009 - 06/2010 As a Helpdesk Engineer, I performed hardware and software installations and provided training, and technical support. Processing on average fifty calls per day to the multiple campuses of CDC (local and global). Created new accounts, conducted account resets and provided efficient support for new employees. Service and maintain network and desktop printers and scanners. Supported multiple software systems: SAS, Citrix, Mainframe and Wireless Support for CDC clients 24 hours a day, 7 days a week. Skills Ability Hard working Diligent Team work Effective communication Punctual compassionate Education Associate of Applied Science in Cyber Security Gwinnett Technical College 2017 Skills FTK, ITIL, METASPLOIT, NESSUS, NIST Additional Information Technology Skills Work in the environments of Windows, Linux, Workstation and VMware physical and virtual Knowledgeable of vulnerability scanning, antivirus components such as Spybot, Emsisoft Toolkit and ClamWin Followed the NIST 800-53 standards and mandated the security policies for the Federal government employees Enrolling employees with PIV Cards through Public Key Infrastructure, and revoking certificates for endusers accounts Enrolling endusers in security environments via Active Directory Implemented Security Training for employees twice a year along with New Hires Definitions were kept update on the servers Work compliance with the SOP Knowledgeable of ITIL best practices Tools Wireshark VMware Microsoft Azure Skype Ivanti Citrix Splunk Metasploit Nessus McAfee NSP WatchGuard SecureTrust Snort Jack the Ripper Aircrack Tcdump Putty FTK Forensic tool ServiceNow SharePoint SCCM LogRythm Symantec Endpoint Console Teniable io Barracuba Application Manager

Name: Carrie Jackson

Email: rodriguezbryan@example.com

Phone: 225.775.3482