Cybersecurity Operations Consultant (Cyber Incidence Response Team) Cybersecurity Operations Consultant (Cyber Incidence Response Team) Cybersecurity Operations Consultant (Cyber Incidence Response Team) - SunTrust Bank Work Experience Cybersecurity Operations Consultant (Cyber Incidence Response Team) SunTrust Bank - Atlanta, GA May 2019 to Present Utilize Falcon Crowdstrike to investigate and analyze malware on endpoint computers and perform network containment of the asset in addition to remotely uninstalling malicious files. Utilize AT&T Luna CDN Service platform to monitor traffic between Akamai DDOS scrubbing centers and our Atlanta and Durham sites. Self-taught Python 3.7.4 programming for the Windows and Python 2.7.2 for Kali Linux environments for penetration testing experience and becoming knowledgeable of hacking tactics and techniques. Utilize RiskIQ to perform analysis of compromised assets and perform preliminary threat hunting. Utilize Splunk 7.3.0 to conduct detailed analysis and correlation of events relating to suspicious activities of computer users Utilize tools such as Arbor Network APS, Shape, ExtraHop and RSA Netwitness to investigate suspicious traffic and packets as well as bandwidth utilization to act as artifacts to support findings in our post incident reports. Unemployed seeking Cyber Security position from 11/2018 to 05/2019 Network Security Engineer III Department of Veteran Affairs HEC Site - Atlanta, GA January 2016 to November 2018 Locate, assess and remediate all network security vulnerabilities on the Department of Veteran Affairs networks and endpoints using VA developed risk mitigation software and NEWT (Nessus Enterprise Web Tool) Assure that all computerized devices and endpoints comply with security standards of the Department of Veteran Affairs federal guidelines. Use WordPress software to build dummy websites for penetration testing purposes. Remediate all vulnerabilities using proprietary CTolZ and dBat applications. Security Engineer II First Data Corporation - Atlanta, GA September 2015 to January 2016 A member of the IAM and SSO team responsible for using Ping Federate to configure IdP (identity provider) or Sp (service provider) connections for in house and client applications. Daily use of Splunk 12.52 to review application server activity monitors and review logs for signs of problems. Liaison Technologies Utilize Tenable Security Center for vulnerability - Alpharetta, GA April 2014 to May 2015 penetration testing coupled with Dell SecureWorks for incident management to better secure the network infrastructure. Travel to satellite offices to configure firewalls, switches, routers, IPS devices, voice gateways in server racks. Mounting of wireless access points. Assisted in the SDLC requirement gathering, implementation and testing phases of single-sign on solutions for application developers using Restful and SOAP methodologies for authentication purposes. Use of Jenkins to assess the security compliance of developers' software applications. In charge of vetting single-sign on (SSO), identity access management (IAM) and multi-factor authentication (MFA) vendors to streamline customer and employee access. Utilize Acunetix WVS 9.5 to scan our public web servers for vulnerabilities and patch/update servers accordingly. Utilization of Algosec Firewall Analyzer to troubleshoot network routing problems and clean up ambiguous and redundant firewall rules. Used Qualys online web scanner to test and grade web facing servers susceptibility to vulnerability attacks. Information Security Engineer Bank of America - Atlanta, GA October 2013 to February 2014 Assist in developing more secure processes and procedures for protecting confidential/sensitive data leaving the banking network and being accessed by 3rd party vendors. Coagulate and organize parallel security project work flows and centralize the information into weekly performance tracking matrices. Troubleshoot VPN issues and perform audits on security appliances and harden them to improve network security. Senior Information Security Engineer Atlanta Public Schools - Atlanta, GA November 2012 to October 2013 Conducted penetration and vulnerability testing using Tenable (Nessus Security Center 4.4.03). Utilized the requirements gathering, implementation and testing phases of the SDLC for the rollout of the district wide rollout of Trend Micro antivirus and virtual station deployment. Created standards, policies and procedures for securing Atlanta Public Schools network infrastructure. Web application firewall proof of concept implementation and configuration. Utilize FTK software to assist with forensics investigations. Monitor, allow and restrict client access to specific websites using IBoss Enterprise SWG Webfilter 14500. Firewall analysis, rule set reviews, work load and services reviews. Hands on working knowledge of load balancing of Citrix Netscaler 11500 appliance during training labs. Detect and discover malware, rootkits and malicious network traffic using Palo Alto 5050 and Dell Sonicwall Next Generation

Firewall IPS devices. Network Engineer Techbridge - Sandy Springs, GA May 2011 to November 2012 Provide remote and on-site technical support at client sites on Windows Servers, Barracuda Spam Filter, Cisco PIX 506e/515e and ASA 5510/5520/5540 firewalls, Cisco ASDM version 6.4, Exchange 2007/2010, Active Directory. Create site-to-site VPN tunnels using IPSec security and Cisco ASA 5510/5520/5540 and PIX 515e firewalls. Create and modify threat signatures with Cisco 4260 IPS sensors. Network Administrator ITT MISSION SYSTEMS February 2011 to May 2011 Monitor network devices with What's Up Gold software and map the Centrix network with SNMPc v2. Add Cisco VOIP phones to SIPR and NIPR networks using Cisco Unified CallManager 7.xxxx Perform network IP subnet segmentation. Configure OSPF, HSRP and EIGRP routing protocols on routers and deploy at various army bases. Performed policy-based routing, summarization, route redistribution, virtual links, stubby and totally stubby networks. System Engineer ALLSCRIPTS - Atlanta, GA July 2010 to December 2010 Contractor) Installed n-tiered healthcare software packages in a mock hospital environment. Used Citrix Xenapp 6 to publish applications on intranet for remote users to access. LAN Engineer GEORGIA DEPARTMENT OF AGRICULTURE - Atlanta, GA June 2007 to July 2010 Configured VLANs and port security for network segmentation and security. Monitor MPLS network traffic and analyze bandwidth usage of local and remote sites with PRTG Traffic Grapher v6.1.0.757 by Paesseler. Perform network IP subnet segmentation. Cisco 5540 Firewall configuration, management and administration. Configured route redistribution between RIP version 2, OSPF and EIGRP routing protocols. Assisted in converting from physical to virtualized environment using VM Ware and ESX Server 3.5 and Linux Microsystem Security Specialist DEKALB COUNTY POLICE DEPARTMENT - Decatur, GA September 2005 to May 2007 Provide end user support for PC-based systems utilized by Dekalb County Police employees. Installed and managed Symantec Anti-Virus software on endpoints and monitored and remediated vulnerabilities. Assist in backing up file servers and rotating tape libraries using Veritas Backup Exec 9.5 and Overland Neo Series 4000 Tape Storage device. Network Engineer THE ONENESS GROUP - Stone Mountain, GA February 2002 to September 2005 Contractor) Accomplishments: Very instrumental part of a team of professionals to convert all telephone systems from analog to digital at Children's Healthcare of Atlanta, Eagleton's and Scottish Rite Hospitals using VOIP (voice over IP) technology. Utilized Cisco Call Manager 3.2 to configure client's voicemail on the VOIP server for the entire hospital campus. Network Administrator GRICE & ASSOCIATES INC - Atlanta, GA June 2001 to February 2002 Installed Exchange 2000 server, web filters, firewalls, antivirus software, and backup/disaster recovery. Performed all 6 phases of SDLC process in the overhaul of the local area network and server installations. Designed, configured and installed a total network solution of a small 50 node client-server local area network with Windows 98, 2000 workstations and a Windows 2000 Dell PowerEdge Small Business Server. Network Administrator GEORGIA ASSOCIATION OF EDUCATORS - Tucker, GA April 2000 to May 2001 Migrated from Banyan Vines/Windows NT platform to 100% Windows 2000 architecture. Installed and managed Enterprise Symantec Anti-virus software on client endpoints to reduce exposure to malware, worms, viruses, etc. Performed all 6 phases of SDLC process in the deployment of Citrix Neighborhood rollout for all offices. Spearheaded the installation of Windows 2000 file servers and Exchange 2000 mailbox servers in conjunction with Active Directory and implementation of SonicWall XPRS firewall. Education Certificate of Information Technology Clayton State College and University December 2004 Bachelor of Civil Engineering in Civil Engineering Georgia Institute of Technology June 1994 B.S. in Mathematics in Mathematics Morehouse College May 1994

Name: Nicole Miller

Email: rickyfox@example.org

Phone: 949.612.9873