Sr. cyber Security Analyst Sr. cyber Security Analyst Sr. cyber Security Analyst - Greendot , Tampa Result Oriented Sr. cyber Security Analyst with 6 years of experience in various aspects of Information and Network Security. Admirable correspondent with analytical, Technical Expertise, relationship management and coordination skills. Six years plus experience in IT Security Operations and implementation, integration & operation. Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements and understanding of NIST and ISO standards. Develop strategic plans for agency-wide implementation to address the operations of client services, product support, quality assurance, and information security training. Technical experience in System and Network Analysis, Intrusion Detection, Malware Analysis Maintained up-to-date procedures and documentation to support IT security processes. Experience and knowledge of threats, analysis, and remediation efforts in reference to Intrusion Prevention and penetrations Experience in Network Intrusion detection/Intrusion Prevention System and Firewalls Experience as a Splunk Engineer configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux environments Providing support to Microsoft Active Directory, Microsoft SCCM servers and SQL servers. Hands-on designing Active Directories using power shell scripts. Responsible for logical and physical database design, implementation, transforming logical data models into physical databases and defining strategies for database implementation, high performance, replication and failover. Hands-on experience on Citrix Provisioning Services,XenApp, App-V, Metaframe PS, XenDesktop and VMware ESX/ESXi Experience with Project documentation tools & implementing and maintaining network monitoring systems and experience with developing network design documentation and presentations using Visio Experience in managing complex routed networks providing technical support, troubleshooting and configuration. Configure, maintain and design network security solutions including firewalls (CheckPoint and Cisco ASA), IDS/IPS (CheckPoint and SourceFire), VPN, ACLs, Web Proxy, etc. Hands on experience on NGFW Firewall management and UTM solutions (IPS/IDS, DLP, Gateway Antivirus, Antispam, Content Filtering, Application

Control) Strong hands on experience on PIX Firewalls Hands on experience on Operations and management of Aruba based wireless network providing multiple SSID platform for DoD users Intrusion Detection- monitor and analyze real time security alerts triggered on the network by Cisco Sourcefire Performed security operations on ASA firewalls. Hands on experience in upgrading and troubleshooting OS for cisco firewalls like ASA and FMC Work Experience Sr. cyber Security Analyst Greendot , Tampa July 2015 to Present Responsibilities: Worked on Cloud Security Products to ensure security of customer from cyberattacks. Knowledge of various DDoS attack types (UDP/ICMP Flood, SYN Flood, HTTP Get Flood, TCP Connection Attack, TCP Flag-based Attacks) Gather information, log, data, investigation, create report. Worked on OWASP TOP 10 attacks like, XSS, SQL Injection, CSRF, PHP Injection etc. Interacation with customer regarding security alerts and attacks. Worked on DDOS mitigation and have good idea on different kind flood attacks. Good knowledge on GRE tunnel , IP sec tunnel, troubleshooting of different issue of tunnels. Experience with Firewall migrations from PIX firewall to Cisco ASA and Juniper SRX firewall appliances. Perform review of raw log files, and data correlation (i.e. firewall, Netflow, IDS, syslogs). Performs vulnerability scans using vendor utility tools. Monitors security audit and intrusion detection system logs for system and network anomalies. Maintains data and communicates to management the impact on business/customer caused by theft, destruction, alteration or denial of access to information. Validates and tests security architecture and design solutions to produce detailed engineering specifications with recommended vendor technologies. Provided remote Technical support on implementation of technology using various Juniper Network & Security products and applications and resolve product related issues through research and troubleshooting. Involved in configuring and troubleshooting Juniper Firewalls including UTM features like anti-virus, deep inspection (IDP), URL filtering and screening. Responsible for Cisco ASA and Palo Alto configuration and administration of networks. Configuring Virtual Chassis for Juniper switches EX-4200, Firewalls SRX-210 Troubleshoot traffic passing managed firewalls via logs and packet captures Involved as Platform Engineer for Sourcefire including all 4.10 and NG and NGFW Integrated web application delivery controller(ADC). Involved in a team responsible

for Network security management by implementing and managing NGFW systems. Virtual Private Networks on Cisco ASAs with AnyConnect, Cisco ISE for authentication, as well as site to site VPN Implemented new Cisco ASA's, installed the framework for Cisco ACI and implemented new F5 LTM's and GTM's. Creating, implementing and testing Citrix NetScaler ADC (Application Delivery Controller) responder policies in order to meet DDoS defense strategies Worked on Converting the Partner IPSEC VPN from one Data Center to Another Data Center Expertise in installing, configuring and troubleshooting Juniper EX Switches (EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series). Performed various configurations using the CISCO SDM like configuring VPN, Security Audits, Firewalls, VLANS. Worked on software based ADC on VMware Responsible in troubleshooting on Cisco ISE added new devices on network based on policies on ISE. Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5585 Security appliance Responsible for Cisco Proxy ESA and WSA. Everyday performance with the Cisco Iron ports - WSA S170 (Web Security Appliance) Version: 8.0.6-119, ESA C370 (Email Security Appliance) Version: 8.5.6-074, and M670 - Content Security Management Appliance Version: 8.3.6-028 Implementation and Configuration (Profiles, I Rules) of F5 Big-IP LTM-6400 load balancers Hands on experience on Web Application Firewalls and attack mitigation techniques. Working in 24 X 7 SOC operations in different shifts. IT Security Analyst - Global Security Operations Health Plan Services, FL January 2013 to June 2015 Responsibilities: Worked on Cloud Security Products to ensure security of customer from cyberattacks. Working knowledge of HTTP(S), TCP/IP , DNS Knowledge of various DDoS attack types (UDP/ICMP Flood, SYN Flood, HTTP Get Flood, TCP Connection Attack, TCP Flag-based Attacks) Gather information, log, data, investigation, create report. Worked on OWASP TOP 10 attacks like, XSS, SQL Injection, CSRF, PHP Injection etc. Interacation with customer regarding security alerts and attacks. Worked on DDOS mitigation and have good idea on different kind flood attacks. Good knowledge on GRE tunnel , IP sec tunnel, troubleshooting of different issue of tunnels. Experience with Firewall migrations from PIX firewall to Cisco ASA and Juniper SRX firewall appliances. Provided remote

Technical support on implementation of technology using various Juniper Network & Security products and applications and resolve product related issues through research and troubleshooting. Involved in configuring and troubleshooting Juniper Firewalls including UTM features like anti-virus, deep inspection (IDP), URL filtering and screening. Responsible for Cisco ASA and Palo Alto configuration and administration of networks. Configuring Virtual Chassis for Juniper switches EX-4200, Firewalls SRX-210 Troubleshoot traffic passing managed firewalls via logs and packet captures Involved as Platform Engineer for Sourcefire including all 4.10 and NG and NGFW Integrated web application delivery controller(ADC). Involved in a team responsible for Network security management by implementing and managing NGFW systems. Virtual Private Networks on Cisco ASAs with AnyConnect, Cisco ISE for authentication, as well as site to site VPN Implemented new Cisco ASA's, installed the framework for Cisco ACI and implemented new F5 LTM's and GTM's. Creating, implementing and testing Citrix NetScaler ADC (Application Delivery Controller) responder policies in order to meet DDoS defense strategies Worked on Converting the Partner IPSEC VPN from one Data Center to Another Data Center Expertise in installing, configuring and troubleshooting Juniper EX Switches (EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series). Performed various configurations using the CISCO SDM like configuring VPN, Security Audits, Firewalls, VLANS. Worked on software based ADC on VMware Responsible in troubleshooting on Cisco ISE added new devices on network based on policies on ISE. Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5585 Security appliance Responsible for Cisco Proxy ESA and WSA. Everyday performance with the Cisco Iron ports - WSA S170 (Web Security Appliance) Version: 8.0.6-119, ESA C370 (Email Security Appliance) Version: 8.5.6-074, and M670 - Content Security Management Appliance Version: 8.3.6-028 Implementation and Configuration (Profiles, I Rules) of F5 Big-IP LTM-6400 load balancers Hands on experience on Web Application Firewalls and attack mitigation techniques. Working in 24 X 7 SOC operations in different shifts. Jr. Analyst - SOC Services Spanco Telecom - IN August 2012 to October 2013 Responsibilities: Managing the service request tickets within the

phases of troubleshooting, maintenance, upgrades, fixes, patches and providing all-round technical support. Commissioning and Decommissioning of the MPLS circuits for various field offices. Preparing feasibility report for various upgrades and installations. Ensure Network, system and data availability and integrity through preventive maintenance and upgrade Troubleshooting complex networks layer 1, 2to layer 3 (routing with MPLS, BGP, EIGRP, OSPF protocols) technical issues. Providing support to networks containing more than 2000 Cisco devices. Performing troubleshooting for IOS related bugs by analyzing past history and related notes. Carrying out documentation for tracking network issue symptoms and large scale technical escalations. Involved in L2/L3 Switching Technology Administration including creating and managing VLANs, Port security, Trunking, STP, Inter-Vlan routing, LAN security. Worked on the security levels with RADIUS, TACACS+. Modified internal infrastructure by adding switches to support server farms and added servers to existing DMZ environments to support new and existing application platforms. Configured switches with port security and 802.1 xs for enhancing customer's security. Validate existing infrastructure and recommend new network designs. Created scripts to monitor CPU/Memory on various low end routers in the network. Configuring and troubleshooting multi-customer network environment. Involved in network monitoring, alarm notification and acknowledgement. Implementing new/changing existing data networks for various projects as per the requirement. Installed and maintained local printer as well as network printers. Education Masters in Computer Science Lamar University 2015 Bachelor of Computer Science in Computer Science Jawaharlal Nehru Technological University 2012

Name: Amber Lee

Email: mccoymichael@example.net

Phone: (797)713-3617x54917