Analyst, Infrastructure / System Engineer - Level 1 Analyst, Infrastructure / System Engineer - Level 1 Analyst, Infrastructure / System Engineer - Level 1 - ACCENTURE AND Microsoft Sterling, VA ? DoD IT 2 Clearance ? CJIS Clearance ? eQip Clearance ? CompTIA Network+ ? ITIL Foundation Certification ? CompTIA Cloud+ Certification ? CompTIA Security+Certification ? Cisco CCNA Certification ? Forensic Eye for Detail. Recognized for noticing minutia that others miss and keenly observing intricate details so as to avoid costly missteps. ? Tenacious Problem Solver. Doggedly determined to research solutions, regardless of time investment, so that the optimal outcome is achieved. ? Flexible Team Player. Committed to going above and beyond core duties to support larger needs of team and ensure that all options have been considered toward goal realization. Work Experience Analyst, Infrastructure / System Engineer - Level 1 ACCENTURE AND Microsoft - Reston, VA 2017 to Present Microsoft group and security policy design and implementation. Ability to analyze and resolve problems associated with server's hardware, applications, and security Troubleshoot using third party diagnostic and monitoring tools, logs, graphs, and performance data to maintain the health and availability of computer systems. Maintain system health, support outage recovery activities and supporting the Microsoft Azure Cloud. Provide a point of escalation and support to the Network Operations Center and Data Center Technicians. Support, maintain and administer third party applications. Produce documentation for application deployment, upgrade, release of new services. System versions, updates and fixes to the cloud environment, and Production System Maintenance activities (Security Patching, Service account maintenance, live escorting, and certificate renewal Cloud Systems Administrator Leidos and Microsoft , Chevy Chase , MD2016 2017 to 2017 Administration of Windows servers, domain servers, supporting desktops, desktop applications, and Active Directory Microsoft group and security policy design and implementation. Ability to analyze and resolve problems associated with server's hardware, applications, and security Troubleshoot using third party diagnostic and monitoring tools, logs, graphs, and performance data to maintain the health and availability of computer systems. Maintain system health, support outage recovery activities and supporting the Microsoft Azure Cloud. Provide a point of escalation and support to the Network Operations

Center and Data Center Technicians. Support, maintain and administer third party applications. Produce documentation for application deployment, upgrade, release of new services. System versions, updates and fixes to the cloud environment, and Production System Maintenance activities (Security Patching, Service account maintenance, live escorting, and certificate renewal Lead Tape/Print Computer Operator IBM-Pomeroy - Sterling, VA 2015 to 2017 Assistant Systems Administrator Cornerstone - Reston, VA 2012 to 2015 100% Load/Unload tapes from ATL File tapes in the vault prepare online documents Required Skills Microsoft Office Suite, Ability to work independently good communications skills, ability to handle oneself professionally. Cornerstone, Reston, VA 2012 - 2015 Assistant Systems Administrator Maintain and administer computer networks and related computing environments for over 150 employees, including computer hardware, systems software, applications software, and all configurations. Perform data back-up and disaster recovery operations. ? Detail Oriented. Maintain a high rate of accuracy and efficiency in completing IT projects. ? Effective Communicator. Work with customers toensure effective data and network security and operations. ? Resourceful. Perform as team leader when needed with managerial and project management responsibilities. ? Problem Solver. Identify problems and perform troubleshooting activities to find root causes and solutions. ? Professional Hands-On Skills Security (CompTIA Security (+) & Certified Ethical Hacking - CEH) Implement security configuration parameters on network devices. Configure firewalls, routers, and switches web security gateways with appropriate network security. Implement common protocols and services such as IPSec, SNMP, SSH, DNS, TLS, SSL, TCPIP, FTPS, HTTPS, SCP, ICMP, IPv4, IPv6, FTP, SFTP, TFTP, Telnet, HTTP and NetBiOS. Understand importance of commonly used ports. Evaluate wireless security protocols such as WEP, WPA, WPA2, 802.1x, EAP, PEAP, LEAP and ECC. Analyze intrusion detection system (IDS) and intrusion prevention system (IPS). Identify detection methods and techniques such signature based detection and anomaly based detection method. For a business scenario secure the organization by applying secure network administration rules. Configure rules for firewall, VLAN and router. Configure access control list, port security and unified threat management. Use network design elements and components to set up

DMZ, subnets, VLAN, NAT, Remote access and virtualized platforms. Troubleshoot security issues related to wireless networking. Identify various control types and risk reduction policies such as mandatory vacations, job rotation, least privilege and Segregation of Duties which need to be applied to ensure risk prevention. Evaluate risk associated with Cloud Computing and Virtualization. Analyze security implications when integrating systems and data with third party vendors / solutions considering factors such as data ownership, backups, policies around unauthorized data sharing etc. For business case, implement risk mitigation strategies such change management, incident management, execution of routine audit and data loss prevention (DLP) controls. Enforce policies and procedures to prevent data loss / theft which included reviewing permission and user access rights on a periodic basis Develop training materials to train user group on importance of security, compliance and best practices such as data handling, clean desk policies and password policies. Provide factors / policies that need to be implemented in physical security and enforcing environmental controls. Develop training materials on various threats, vulnerabilities and attacks. Evaluate mitigation controls and deterrent techniques that must be used for various attacks. Evaluate various tools and techniques that can be used to analyze threats and vulnerabilities. Use techniques such as penetration testing and vulnerability scanning to analyze security threat / vulnerability. Understand various security controls and policies that need to be implemented for application, mobile, operating system, virtual environments, cloud and portable devices Evaluate authentication, security and access controls for an organization based on various authentication factors, identification, and privilege assigned. Analyze cryptographic methods, PKI and certificate management to implement digital certificate and trust models Networking (Cisco Certified Network Associate - CCNA) Identify importance and functionality of various network devices such as routers, switches, bridges and hubs. Determine components required to meet network specification and for successful operation of common application on the network. Understand concepts related to basic operation of protocols in OSI and TCP / IP Models. Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN Determine technology and media access control

methods for Ethernet networks. Identify basic switching concepts and operation of Cisco switches such as Collision Domains, Broadcast Domains, ways to switch and CAM Table Verify switch configuration such as hostname, mgmt. IP address, IP Default gateway, username, password, console, VTY login and service password encryption. This verification process also includes review of remote access management Verify network status and switch operation using utilities such as ping, telnet and SSH. Understand importance of VLAN and configure them to create logically separate network and manage traffic. Configure interVLAN routing and SVI interfaces. Configure trunking of Cisco switches as well as PVSTP operations such as root bridge election and spanning tree mode. Identify appropriate IPv6 and IPv4 (VLSM) addressing scheme to satisfy requirements in a LAN/WAN environment. Identify technological requirements for running IPv6 in conjunction with IPv4. Configure basic router configuration and verify network connectivity using Telnet, traceroute, SSH and ping. Determine methods of routing and routing protocols. Configure DHCP (IOS Router), Access Control List, NAT, NTP and syslog for a given network. Troubleshoot issue related to network, network traffic, VLAN, interVLAN, spanning tree operation and WAN. Practical experience through use of software / tools to analyze security, network and vulnerabilities: ? Assessing and Securing Systems on a Wide Area Network (WAN) ? Applying Encryption and Hashing Algorithms for Secure Communications ? Analyzing Network Traffic to Create a Baseline Definition ? Data Gathering and Footprinting on a Targeted Website ? Auditing a Wireless Network and Planning for a Secure WLAN Implementation ? Attacking a Vulnerable Web Application and Database ? Identifying and Removing Malware on a Windows System ? Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation ? Investigating and Responding to Security Incidents ? Securing the Network with an Intrusion Detection System (IDS) Education Masters of Science in Computer Security in Cybercrime Security, Web Application Security, Security Strayer University - Ashburn, VA 2014 Bachelor of Science in Information Systems and Management University of Potomac - Herndon, VA 2009 Skills ACTIVE DIRECTORY, VLAN, NETWORKING, SECURITY, NESSUS

Name: Ashley Cisneros

Email: ibarradanny@example.org

Phone: (649)762-4776