Cyber Security Engineer Cyber Security Engineer Cyber Security Engineer - Kintetsu Global IT Apt, AR Authorized to work in the US for any employer Work Experience Cyber Security Engineer Kintetsu Global IT - Farmers Branch, TX August 2018 to Present   Assist the Cyber Security Manager with the development of Security Procedures, and Work Instructions   Tracks performance metrics and provides timely updates to management   Develop, improve and help implement best practices for risk reduction across a broad range of enterprise applications, systems, networks and interfaces   Assists with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions   Works with clients to implement system security measures, assists with computer security plans and documentation and provides technical guidance and training   Perform network traffic analysis using raw packet data, network flow, Intrusion Detection Systems (IDS), and custom sensor output from communication networks   Scheduled daily security reports for managers, engineers, shareholders   Ran vulnerability test (Ethical Hacking) against corporate network i.e. servers, switches, servers.   Remediate any Security Alerts i.e. Port Blocking, Blacklist, Creating Policies on Firewall.   Work with developers, system/ network administrators, and other associates to ensure secure design, development, and implementation of applications and networks   Performed Security Device firmware upgrades   Performed Network, Data Forensics to determine any possible Attacks, Threats, Vulnerabilities using SolarWinds Security Event Manger and SolarWinds Orion. Determine Correlation with threat and outages.   Tested EC2 Instances in AWS with Cloud Security   Tested and deployed Server root certificates for authentication and security purposes.   Deployed, Maintained, Configure SolarWinds agents on Servers and Network devices for activity, security, reporting purposes. MSP NOC Engineer Konica Minolta All Covered MSP January 2018 to January 2018 June) - Insight Global - Konica Minolta All Covered MSP (Contract)   Monitor Network Critical, High, Low Outages Alerts using Solar Winds MSP   Remediate Issue Citrix, VM Ware, MS Server 2003, 2008, 2012, Cisco, Fort iGATE   Utilized remote tools using Bomgar, Kaseya, Nable to remediate client issues   Administered, Maintained Active Directory Services   Administered and Maintained Microsoft Exchange, Office 365   Remediated Server Performance issues, High CPU, High Memory, Low

Disk Space   Remediated Desktop, Application and Performance Issues. Network Operations Center Tech June 2017 to June 2017 DEC) TEKsystems- AFL- Wells Fargo Data Center (6 month Contract)   Racked and stacked Network devices, Switches, Servers, Fiber Extenders, Routers, Firewalls, Security devices.   Ran Fiber Infrastructure Trunks, Fiber connections, Copper Cat 5e, Cat6, Cat6a   Troubleshoot Infrastructure Connections using VFL, Toners, and Cable testers. Decommissioned Network Devices and prepped for salvage.   Built Network Cages and prepped for device installation.   Site Validation, surveyed network paths for preparation for upcoming network jobs. Network Technician TEKsystems April 2016 to January 2017 Arizona State University Network Conversion Project.   Site survey for preparation for Cat3 to Cat6 conversions.   Activated Connections from patch panels to Cisco switches   Scanned Cisco network switches for open ports using cisco command, ex CDP commands.   Assigned VLANS, Port security, Trunking, port speed Monitor Solar winds, Cisco Prime, for down devices.   Utilized IPAM for ip address block, open for assignment.   Configured and installed Cisco switches 3900 series and 2900 series cisco POE and non POE switches. Using command line interface, cisco IOS. TFTP configurations.   Set up wireless access points.   Full building switch audit for documentation   Troubleshoot network issues. Connections, Configuration, etc. Network Analyst Presidio - Chandler, AZ August 2015 to March 2016   Upgraded Cisco IOS on Switches   Configure Cisco ASA 5505-50   Created Vlans, Switch Access Ports, Security   Monitored Network Activity using Cisco Prime 2.2, Splunk, Ops Manager, IPAM, Wire Shark   Created Technical Document SOP, Reference Guides, Work instructions in compliance with the ITIL standardization.   Created port mapping Network Diagram Created Network Topology using Visio   Configured and Deployed 100 plus catalyst and access switches to various sites.   Racked and Stacked Routers, Switches, Firewall   Troubleshoot issues with switched network ex switch stack config, subnet issues, and protocol issues.   Wipe configuration on Cisco core 4507, 4600, 3750 series. Deleted Vlan configs, Passwords, interface info, protocols, etc.   Documented inventory on deployed and decommissioned network equipment. Network Administrator/Desktop Support Cook Native Ministries - Tempe, AZ 2014 to 2016 Managed Html website www.cooknam.org   Supported end users with Laptops, Desktop, Printer

issues.   Establishes and maintains user accounts, profiles, file sharing, access privileges and security (AD)   Managed IP phone systems   Maintained relationship with vendors such Dell, HP, Microsoft for hardware and software needs for the company.   IT inventory management and control.   Maintained back up of data.   Implemented network, data secure practices.   Provided remote support for telecommuters SOC Analyst Scottsdale, AZ 2015 to 2015 Terra Verde-(Aug) (Jan - August) Project   Monitored network security events received from customer's monitored servers, Scottsdale, AZ And then take appropriate action based on customer's security policy. Operated Alien Vault SEIM consoles in order to monitor the environment for events of interest Monitored Cisco ISDM   Analyzed cyber-attack methods such as SQL Injection and Cross Site Scripting attacks (XSS.)   Network protocols used TCP/IP, UDP, DHCP, FTP, SFTP, ATM, SNMP, SMTP, SSH, SSL, VPN, RDP, HTTP and HTTPS.   Use vulnerability assessment data to pinpoint potential points of attack   Executed incident response process when a security incident has been declared   Analyzed vulnerabilities using SNORT Network Intrusion Prevention System. Network Security Analyst InfoSec - Scottsdale, AZ 2015 to 2015 Terra Verde- PayPal/EBay Project (Jan-August)   Configured and Deployed Tripwire Ip360 Security Device all throughout PayPal/EBay Network   Scanned IP Network, Servers Unix, Windows, Desktop, and Laptop for Threats and Vulnerabilities using tripwire ip360 and Qualys technologies.   Reported Threats and Vulnerabilities using CVE score and National Vulnerability Database guidelines and Risk Calculator.   Designed and Implemented Network Structure coverage within Tripwire ip360 VNE and Device profiles.   IT audits using spreadsheet to keep track of IP coverage and physical security device on the network.   Calculated IP Range Coverage using IP Calculator.   Monitored Security Threats for PCI compliant Networks. Jr Systems Administrator/Application Support Service King - Scottsdale, AZ 2013 to 2014 Hardware/software support, training, and special projects (Server 2008, Exchange, IIS, DHCP, DNS, Active Directory, Lync, and Kace Server)   Supported data connectivity for local area network (LAN) and wide area network (WAN) systems   (Cisco 2900, Cisco Catalyst 3560, Cisco AIR-LAP1262N-T-K9 802.11a/g/n)   Assisted in coordinating special projects including network related wiring plans, LAN/WAN hardware/software purchases, and system installation,

backup, maintenance and problem solving; assists in providing network and remote connectivity hardware/software support   Maintained LAN user documentation including hardware/software applications, support logs and other related information   Assisted in installing, designing, configuring, and maintaining system hardware and software   Analyzed and troubleshoots the network logs and tracks the nature and resolution of problems and monitors usage to ensure security of data and access privileges   Establishes and maintains user accounts, profiles, file sharing, access privileges and security (AD)   Established and maintained user e-mail accounts and provides e-mail training and software support(Exchange)   Managed anti-spam and anti-virus servers (AT&T and Microsoft Forefront)   Coordinates the ordering and installation of telecommunications and data systems equipment and cabling   Researched, analyzed, troubleshoots and resolved telecommunications related problems   Created and/or modified voicemail and call features; installs telecommunications equipment and provides support for handsets, voicemail and new/emerging telecommunications-related technology (AVAYA) Education Bachelor of Applied Science degree in Operations Management Arizona State University December 2004 Associates in Applied Science in Cisco and Microsoft Networking Technology Chandler Gilbert Community College Skills Cyber Security, Information Security, Nist, Siem, Network Security, Cybersecurity, It Security, Linux, Information Assurance, Comptia Additional Information WINDOWS 10, WINDOWS 7, WINDOWS SERVER 2008r2 and 2012, ENTERPRISE SERVER 2008, IIS 7, ACTIVE DIRECTORY, EXCHANGE, VPN, REDHAT LINUX 7, ETHERNET, CISCO ROUTERS, PALO ALTO FIREWALLS, CISCO FIREPOWER. FTP, SFTP, SSH, VPN, ORACLE VIRTUAL BOX, VMWARE, FORTINET. CISCO IOS XE, CISCO ASA, SOLARWINDS SECURITY EVENT MANAGER, SOLARWINDS ORION, LINUX CENTOS 7, KALI LINUX, GNS 3, PUTTY, FILEZILLA, WINSCP, DNS, DHCP, AMAZON WEB SERVICES, LAMP, NAGIOS, WEB HELP DESK

Name: Susan Knight

Email: raymondrodriguez@example.org

Phone: 6375094585