Vulnerability Management Analyst Vulnerability Management Analyst Vulnerability Management Analyst - Insight Global (JFHQ-DODIN) Jessup, MD Work Experience Vulnerability Management Analyst Insight Global (JFHQ-DODIN) February 2019 to Present Review, correlate and report on high priority DoD threats and vulnerabilities that impact or target the DODIN Develop consolidated notifications and updates for threat and vulnerability activity Release situational awareness reports, operational directives/orders for quarterly threat analysis reports and metrics Review, analyze, and maintain the content of the DoD database to aid in the detection and mitigation of threat activity Update DoD shared situational awareness mechanisms including websites, Wikipedia, and collaboration forums Develop and present cyber threat briefings and presentations to leadership to ensure situational awareness and status are conveyed Operate as the DoD community leader for the discovery of threat activity and associated indicators Determine sophistication, priority, and threat level of identified malware and intrusions Develop metrics and trending/analysis reports of malicious activity used to compromise the network Manage a DoD prioritization process to identify priority threats and vulnerabilities that are impacting the network Information Security Analyst ICF International November 2017 to Present Installing HBSS modules: McAfee Agent (MA), Host Intrusion Prevention (HIPS), Virus Scan Enterprise (VSE), Policy Auditing (PA), Data Loss Prevention (DLP), Rogue System Detection (RSD), Asset Baseline Monitor (ABM), and Asset Configuration Compliance Module (ACCM). Performed Vulnerability Assessment scans using ACAS (Assured Compliance Assessment Solution) ACAS Security Center, and Nessus scanners. Troubleshoot user COTS software and hardware related issues Manage user accounts via McAfee ePO 5.3.1 Manage MS Outlook accounts and distribution lists Ensuring Command Cyber Readiness Inspection (CCRI) compliance with applicable Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs). Monitoring HIPS and VSE event logs, conducted ongoing risk analysis and policy tuning. Configure, Install, Monitor and troubleshoot Operating Systems on VMware 6.5.0 virtual machines Utilize Remedy ITSM to manage IT service requests. Develop network stoppage, and compliance reports to present to senior leadership Utilize SCAP tool for STIG and vulnerability

assessment and compliance Generate reports via ITSM Remedy for weekly and monthly metric reporting Ensure program, and asset compliance by scanning for vulnerabilities Conduct weekly meetings with the Program Managers to ensure that all personnel involved with Program development, and COOP, are conducting proper testing, notification, and with adherence to STIG compliance. Systems Administrator Chameleon Integrated Services (DISA) April 2015 to November 2017 Install, Configure, Monitor and troubleshoot Microsoft server 2008r2/2012/2016 Monitor server performance, health and event logs with Splunk Troubleshoot user COTS software and hardware related issues Manage user accounts via Active Directory Manage MS Outlook accounts and distribution lists Ensuring Command Cyber Readiness Inspection (CCRI) compliance with applicable Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs). Configure, Install, Monitor and troubleshoot Operating Systems on VMware 5.5 virtual machines Troubleshoot user accounts utilizing Active Directory Utilize Remedy ITSM to manage IT service requests. Manage DISA CONUS Server connection utilizing Solarwinds monitoring tool Systems Administrator Defense Spectrum Organization January 2014 to April 2015 Utilize Remedy ITSM to manage IT service requests Download and install Microsoft patches from WSUS server every Wednesday Install and Maintain virtual machines on ESXi Server Scan devices using SCAP tool for vulnerabilities Prepare reports and maintain records of work accomplishments to communicate work related information to management. Document and track Action Items in MS SharePoint Maintain system backups using SL500 tape library using Symantec NetBackup 7.0 Make changes to group Policies using Regedit Download patches/updates to comply with IAVA's from ACAS and Retina scans Manage mission user accounts with Active Directory Manage DoD PKI systems for CAC issuance and pin resets Enforce all group policies requested by Security Officers according to DISA IA STIG's Update McAfee Anti-virus DAT files on a weekly basis Assist Network Engineers with hardware configurations (IP and MAC addresses) Tier 3 Help Desk Technician Ace Info Solutions February 2013 to January 2014 Troubleshoot all aspects of Windows XP, Windows 7, MS Office, Internet Explorer, and proprietary software, especially client/server based applications, database clients and

web based applications Excellent customer service skills and focus Ability to troubleshoot all aspects of network connectivity from the desktop Excellent written and oral communication skills Ability to work independently with minimal supervision Ability to work as part of a cohesive highly skilled and motivated team Experience with system configuration and setup in windows Knowledgeable of Active Directory Provide Tier 3 help desk support Support Help desk with performance metrics and other reporting support Supported application release deployments Support SIPR operations at client site Level 2 Help Desk Technician Hewlett Packard - Packard, WA April 2012 to February 2013 Remote and customer facing support for end users Add users to the network utilizing Active Directory Troubleshoot account issues utilizing Active Directory Provide day to day remote VPN support for end users Utilize Remedy and SM7 ticketing systems Install and/or troubleshoot VPN application with air cards Install and/or troubleshoot blackberries w/ CAC authentication Support equipment and software moves/adds/changes Add users into the SharePoint environment through Active Directory Technical support of workstations, laptops, printers, smart phones and all peripheral devices Tier 1 IT Help Desk Walter Reed National Military Medical Center August 2011 to April 2012 Remote workstation support using Dameware application Create user accounts utilizing Active Directory Provide day to day remote VPN support for end users Microsoft office application suite support Add/ remove users to SharePoint sites also set permissions for existing users Install and repair VPN application for end users Software installation and troubleshooting Added users into the SharePoint environment through Active Directory Security software installation and updates Log helpdesk trouble calls using isupport ticketing system in the call center Skills Active directory, Encryption, Remedy, Vmware, Disk encryption, Netbackup, Symantec, Ms office, Hyper-v, Windows 10, Windows 7

Name: Daniel Miller

Email: anaperez@example.org

Phone: 001-288-932-3150x238