Security Analyst Security Analyst Security Analyst Montgomery Village, MD Authorized to work in the US for any employer Work Experience Security Analyst Convergenz December 2018 to Present Proactively search for and respond to security events and incidents from SIEM, Firewall (FW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Antivirus (AV), Network Access Control (NAC) and other client data sources ? Use strong TCP/IP networking skills to perform network analysis to isolate and diagnose ? Develop and Adjust SIEM rules and analyst response procedures ? Identify IOCs and add them to active list ? Perform analysis on IDS logs as well as a packet trace/capture logs ? Escalate incidents and act as a Security Incident Response Team Lead when necessary System Security Administrator Walter Reed National Military Medical Center October 2016 to December 2018 Administers day-to-day PACS operation and maintenance, manages and monitors overall system performance, and performs regular checks to ensure smooth workflow from multiple modalities to the PACS system. ? Lead remediation efforts and delegate to project teams ? STIG implementation and vulnerability mitigation (CAT 1's, CAT 2's, etc.) for both servers and workstations within the PACS radiology environment. ? Create and submit POAMs, Security Exceptions, and PPS requests when required ? Support ongoing Risk Management Framework (RMF) and ATO process System Admin/Jr Security Admin P3S Corp August 2012 to October 2016 Maintain mission-critical systems utilizing VMware vCenter/vSphere ? Remediate CAT's I, II, III vulnerabilities for Both Backend servers and Desktops ? Maintain mission-critical systems and applications at highest DoD standards for security and availability utilizing STIG's to build and configure windows server environment. ? Manage and train Helpdesk Technicians ? Leverage performance and alert monitoring tools like NagiosXI, SolarWinds LEM & Splunk to maximize enterprise reliability and troubleshoot network related issues. ? Responsible for implementation, testing and training of new enterprise projects and initiatives. NOC/VoIP Analyst (CWPS) USCG Headquarters January 2012 to August 2012 working at USCG Headquarters ? Manage and troubleshoot Cisco switches ? Configure, update and edit Cisco and 3COM PBX and VBX ? Run, terminate, and test CAT5e Cable ? Perform cable management ? Troubleshoot Cisco and 3COM VoIP Phones IT Specialist August 2011 to January 2012 Eminent, IT-Short term);

Working at WRNMMC (NMPDC) ? Provided technical support to over 300 Users ? Telework Administrator: Imaged, encrypted and deployed over 100 laptops ? Created and maintained user accounts in Active Directory ? Performed Data Recovery using R Studio Education High school or equivalent Skills DNS, DHCP, VMWARE, NESSUS, NMAP, SPLUNK, WIRESHARK, ENCRYPTION, LINUX, SYMANTEC, WINDOWS SERVER 2008, WINDOWS XP, security, access, Active Directory Certifications/Licenses Splunk Core Certified User Present CCNA Cyber Ops April 2018 to April 2021 ECCouncil CEH April 2017 to April 2020 CompTIA Security+ CE June 2021

Name: Walter Norman

Email: robertmckay@example.org

Phone: 3958512540