NDWO Analyst NDWO Analyst NDWO Analyst - Defense Information Systems Agency Fairfax, VA Authorized to work in the US for any employer Work Experience NDWO Analyst Defense Information Systems Agency January 2018 to Present Pending) (On Orders) * In the support of Joint Service Provider (JSP), serve as a single point of entry and dissemination for IA, CND and Cyber Security related information, tasking, orders, alerts, warnings, notices and products * Serve as a single point of exit to report on the same information to higher headquarters to include any Requests for Information (RFIs) * Maintain situational awareness on the status of all security related developments, tasking, orders, alerts, warnings, notices and products * Serve as the primary liaison within the CND division and coordinate with other JSP divisions, the JSP NOC Battle Captain, DISA, JFHQ-DoDIN, USCYBERCOM, other TIER II organizations, and tenant organizations * Consolidates trending of cyber security metrics and creates the products that are required for briefing leadership, partners, and customers regarding computer network defense. * Higher level reporting requirements for DISA, JFHQ-DoDIN, and CYBERCOM * Classified Spillages and Unauthorized Cross Domain Connections * Creating and following TTPs for Cyber Incident Tracking and Reporting * Create CND Metrics per contractual agreement and post to appropriate portals * Reporting changes to the INFOCON status * Ensure readiness of CND Security Tools * Provide daily reports of the current operational status for PENCIRT * Create Commanders Critical Incident Reports if any incident should occur * Research cyber legal concerns per request * Provide clarity to ambiguous ORDERS through the RFI process * Provide OSINT to CSC Leadership areas of interest Network Warfare Operator 143rd Cyber Warfare Company June 2017 to Present * Provide crucial intelligence and network support for defensive and offensive cyber operations * Collect, analyze and report cyber intelligence * Maintain network defense tools, configurations of security appliances and testing infrastructure for operations * Evaluate network defense operations * Provide Cyber Threat Intelligence support for operational teams * System engineering and administration of windows and Linux based O/S * Assisting in the creation of a virtualized Data Center (private cloud) * Hardening virtualized environments with best security practices * Detection, Acquisition, location and identification of foreign electronic intelligence *

Exploited non-voice communications and other electronic signals to provide strategic/tactical intelligence * Operated signal intelligence software and prepared logs/reports * Performed basic signal analysis to determine signal parameters Security Specialist Cyber Brigade S October 2018 to September 2019 * Assisted in the development, build out, and administration of a green field hyperflex data center * Provided project support related tasks to integrate security platforms as well as ongoing tuning support for existing technology * Maintained the security services and technologies involving the SIEM configuration & planning, and incident response * Lead incidents, coordinating and directing multiple subject matter experts internal and external to the organization * Specialized in network centric analysis utilizing a variety of tools and techniques such as Network Security Monitoring, log analysis, and more * Technical leadership guiding the development and evolution of our security monitoring platform as well as detection and response procedures * Provided training and mentoring of junior and mid-career team members * Responsible for providing Security Architecture services during normal business hours * Utilizes digital forensic tools including ThreatGRID Advanced Malware Protection (AMP) and Firepower management console (FMC) to execute digital investigations and perform incident response activities * Perform hunting for malicious activity across the network and digital assets * Conducts analysis using a variety of tools and data sets to identify indicators of malicious activity on the network * Collaborates with technical and threat intelligence analysts to provide indications and warnings, and contributes to predictive analysis of malicious activity * Detonate malware to assist with threat research * Established links between suspects and other violators by piecing together evidence uncovered from a variety of sources * Established and maintained defensible evidentiary process for all investigation * Checked for updates and upgrades, apply patches, and maintain security appliances. * Built up ESXI hosts for DevOps stack on Dell Servers and networked iDRACs * Deploy Vsphere and build required VMs and servers * Wrote Powershell scripts for AD administration for Azure Cloud Office 365 accounts as well as normal active directory * Responded to helpdesk tickets and SCRUM tasks created in JIRA * Created a knowledge based articles utilizing Confluence PPSM Analyst 143rd Cyber Warfare Company June 2017 to January 2018 *

Ensure that all Enterprise Information System Ports, Protocols, and Services (PPS) are registered in the PPSM central registry * Ensure that all PPS are categorized and updated on the PPSM Category Assurance List and are not deployed prior to approval from the Authorizing Official (AO) * Assist the government to develop, revise, implement, and enforce PPSM policies * Validate information in DoD databases and Web sites, including Systems and Network Approval * Process(SNAP), SIPRNet GIG Interconnection Approval Process (GIAP) System (SGS), and Ports and Protocols System Management (PPSM) database VTC Technician February 2017 to June 2017 * Troubleshoot Tandberg video conferencing equipment * Establish SOPs for use of conferencing facilities and equipment * Troubleshoot Lan and ISDN based video equipment * Provide on-site technical support for VIPs during teleconferencing calls * Orders and Tasking Compliance Windows 10 Migration Technician November 2016 to February 2017 * Image PC's, laptops, printers for Windows 10 Migration * Wiped retired equipment * Responded in a timely matter to tickets and work orders * Conducted on-site repairs for internal customers in a Windows environment * Troubleshoot to diagnose issues; replace/swap out equipment * Provide hardware support on laptops, desktops, and tablets * System imaging and deployment, refresh and upgrade projects * Followed all quality processes required * Imaged computer equipment for internal and external customer and related peripherals * Understanding of and working with warranties * Demonstrate attention to detail and ability to follow documented procedures * Documentation of work-flow PMO Analyst Flavell Divett Mountfield Group May 2016 to October 2016 * Graduated top of my class in Project Management Office/ Application Support Role * Utilized SQL to update and query financial tables with correlated and non-correlated subqueries, sequences, views, Data Markup Language, Transaction Control Language, Data Definition Language and Data Control Language on an Oracle 11g Relational Database Management System * Utilized pivot tables, aggregation techniques, and Vlookup/Hlookup in Excel for precise graphical displays of money markets and organization structures * Wrote Procedural Language / Structured Query Language(PL/SQL) procedures for a stock market database to return desired queries on prices, locations, trades, markets, companies, brokers, and holders while updating needed stock related tables IT Technical Level Intern Federal

Energy Regulatory Commission - Washington, DC August 2015 to December 2015 * Produced the artifacts for a successful audit * ensured the availability of E-Library internal and external to assist tier 3 tier application support / network support. * Collected customer and technology information to determine technical support level; elevate calls to appropriate support level as necessary * Solved network connection issues with onsite facilities crew and remote administrators IT Help-Desk Customer Service Representative Cegedim Dendrite - Chesapeake, VA December 2014 to July 2015 * Reduced the number of missed calls while exceeding SLA quality levels to avoid breaches of contract throughout the duration of employment * Provided business-clients with efficient support - Responded to phone calls, emails, and in-person requests in relation to IT service requests * Supported customer requests via telephone, email, fax, or other available means of contact to the Support Center * Assessed the user's issues and provides first level support for problem resolution * Documented client related issues in Remedy and ServiceNow specific to the resolution and escalated unresolved issues expeditiously to the appropriate queue * Recognized operational challenges and suggested recommendations to management in relation to new and ongoing issues * Troubleshoot Mobile Device Management software MobileIron for IOS products * Used WebEx and Jabber to communicate and remote into client's computers * Performed account administration with Active Directory to edit email addresses, update distribution lists, change domain for users, and reset passwords * Worked in multiple environments using VMware technology * Supported Veeva CRM through Salesforce Platform and performed limited administrative duties including adjusting views, updating user information, and password recovery Education High school or equivalent Skills training, database, Management, Excel Certifications/Licenses Security+ March 2017 to March 2020 Certified Ethical Hacker (CEH) June 2019 to June 2022 ITIL v3 May 2015 to Present Splunk Core Certified User July 2019 to July 2021 Foundation certificate in business analysis July 2015 to Present Signal intelligence collection May 2019 to Present 35S MOS training

Name: Steven Meadows

Email: moorefernando@example.org

Phone: 001-241-606-4006