Security Analyst Security Analyst Security Analyst - Defense Software Corporation Inc Organized analytical IT professional with proven experience, valuable decision-making skills, and quality problem-solving skills. Solid reputation for ambitious work ethic, positive mental attitude, and a broad technical knowledge. Proficient at monitoring technical support operations, ability to diligently troubleshoot issues to identify root causes, knowledge of preventative maintenance measures to keep network safe, quality customer service and ability to keep pace with constant cyber threats and evolving security needs. Work Experience Security Analyst Department of State/Diplomatic Security April 2018 to Present * Conducted RMF steps 1-3 Categorization, Selection, Implementation of security controls pursuant to NIST SP 800-37. * Recommended system enhancements to improve security deficiencies in applications. * Conducted pre-assessment documentation preparation for applications undergoing a software deployment (PCCA, NOC). * Assessed enterprise applications to ensure completeness of applicable NIST controls according to the SCF (system categorization form) of the system. * Participated in ACA (Annual Control Assessment) * Verified and updated security artifacts as needed to ensure applications are NIST complaint. * Provided information assurance support for the development and implementation of security application architectures to meet new and evolving security requirements. * Advised and assisted with the Lifecycle Assessment and Authorization (A&A) process and development of Systems Security Plan (SSP) * Ability to track, create and manage information technology (IT) weaknesses, Plan of Action and Milestones (POA&M), utilizing the XACTA. * Comprehensive knowledge to identify hybrid, inherited, common and system level controls * Reviewed and updated ISCP (Information System Contingency Plan) * Identify common threats, vulnerabilities and supported security control baselines to achieve FISMA compliance * Review Security Authorization documents for integrity and completeness with respect to testing and risk analysis * Ability to interpret security requirements into technical solutions and analyze system configurations to determine security posture IT Specialist/LAN Administrator Foreign Service Institute May 2017 to April 2018 * Knowledge of industry accepted standards and best practices. * Communicated with state department personnel about potential phishing and social engineering attacks which could cause

untold damage to security posture. * Ensured state department personnel were complying and up to date on cyber awareness training. * Assisted incident handler with cyber incident response (security infractions), including mitigation, triage and reporting in which corrective actions are recommended to management and DOS CIRT group * Identify, track and remediate vulnerabilities identified by security tools or ISSO. * Assisted ISSO in vulnerability scans using IPOST to ensure risk analysis score on all workstations are following security posture. * Utilized IPOST to manually patch machines that were not updated/offline. * Utilized Nmap to scan network topographies to fully audit and assess the overall security of systems and applications within network topology (testing environment) * Assisted ISSO with updating McAfee anti-virus definitions of more than 500 systems. * Assisted CIRT with patch management and mitigation of ransom ware virus, wanna-cry virus, S-delete. * Knowledge of various Nmap scans conducted in CEH virtual environment (Full scan, half scan, idle scan, xmas scan) * Solid understanding of OSI model, CJCSM, NIST and STIGs.. * Knowledge of IDS, IPS, WIPS, WIDS. (behavior and differences) * Experience reviewing network traffic using Wireshark 2.4.6 in home office and CEH virtual environment. * Functional knowledge of firewalls, routers and network appliance. Tier II Help Desk Specialist (Subcontractor) DOD Pentagon November 2016 to April 2018 * Provide 24/7 Tier II technical support to the DoD, US Army, and other government agencies * Instruct users with proper hardware and software utilization * Install approved software and performed hardware troubleshooting. * Responded to inbound calls/emails in a timely and professional manner * Document all interactions in the remedy tracking system and escalate issues that cannot be resolved in a timely manner. * Performed CAC pin resets and unblocked CAC cards as a registered TA. * Troubleshoot all MS Office issues to include Outlook * Re-imaged desktops/laptops/tablets with windows 7 & 10 using SCCM. * Mapping of network drives, identify corresponding file share, and map network printers. * Assist customers with account creations across multiple applications and follow designated escalation procedures when necessary Mind Finders August 2013 to November 2016 * Re-imaged desktops/laptops (windows7) * Mapped network printers for users/creating script files * Performed on-site support and provided remote support to off-site customers * Utilized ticket system to document and record trouble tickets.

* Manage the processing of incoming calls to the Service Desk via both telephone and e-mail and to ensure courteous, timely, and effective resolution of end user issues. * Monitor and test resolutions to ensure problems have been adequately resolved * Contributing to and updating knowledge base content built on the problem resolution and training * Assisted with asset management including tagging and tracking of inventory Education A.A.S in Information Technology in Information Technology Prince George's Community College - Largo, MD Skills Active directory, Dns, Networking, Remedy, Snort, Splunk, Vpn, Wireshark, Dhcp, Ldap, Tcp, Udp, Iphone, Linux, Lan, Microsoft office, Windows 7, Training Additional Information & COMPETENCIES Software * Windows 7/10, Kali Linux (beginner) * Microsoft Office 365, Microsoft Office 2013/2016 * VDI * Dame ware, Windows Desktop Remote * Remedy Ticking System * Norton Anti-virus * Mobile configuration (iPhone, Samsung, Black Berry) Networking * Active Directory, DNS, DHCP, LDAP * VPN, * LAN, WAN, TCP, UDP * OSI model * 3-way handshake Tools * Wireshark * Burp Suite * OWASP ZAP * VEGA * XACTA * SNORT (beginner) * Splunk Enterprise Fundamentals Training * Cybrary Virtual environment (practicing ethically)

Name: Thomas Young

Email: sara82@example.org

Phone: +1-243-647-8791