IT Security Analyst IT Security Analyst IT Security Analyst - CWorld Security LTD Silver Spring, MD LOOKING TO OBTAIN AN IT SECURITY ANALYST POSITION IN A FAST -SPACE ORGANIZATION WHERE EXCEPTIONAL SKILLS AND ABILITY WILL BE USEFUL TO MEET SET ORGANIZATIONAL GOALS. 5 years of Experience Work Experience IT Security Analyst CWorld Security LTD July 2016 to Present Duties included: ? Support client with documenting and reviewing security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies. ? Support Client in conducting Vulnerability Scanning using NESSUS, Web Inspect and Nexpose ? Supporting client with internal facilities and systems security control assessments (SCA) for Pre-OIG efforts. ? Supporting BRT in conducting POA&M quarterly reviews as part of POA&M remediation. ? Reviewing Open and Closed POA&Ms for GSS systems and facilities. ? Conducting Security control evidence reviews for client facilities and system as part of POA&M remediation. ? Supporting client in conducting internal security control reviews and drafting observation and recommendations ? Supporting Client in Creating POA&Ms after assessments as part of Pre-OIG Efforts ? Supporting client facilities in travels, conducting internal security control site assessments for facilities as part of the VA Pre-OIG Efforts. ? Assist client facilities in the creation of new findings uncovered during internal security control assessments. ? Assess the Cyber Security risk of IT systems documenting them in formal risk assessments and supporting artifacts associated with the Assessment & Authorization (A&A) process. ? Organizes, develops, and presents briefings, written summaries, and written reports incorporating narrative, tabular and/or graphic elements. ? Implements IT security solutions and assures successful implementation. ? Analyzing Vulnerabilities from Security Assessment Report and drafting remediation strategies. ? Creating Findings from SAR in order to mitigate weaknesses as part of POAM remediation. ? Supporting client in reviewing, updating and developing security artifact as for compliance accuracy and completeness such as SSP. SAR, SAP, POA&M, CP, BIA, PTA, PIA, RA, ISA, IR, DRP, MOU and SLA. ? Perform specific quality control for packages validation on the SP, RA, RTM, PIA, SORN, E-auth and FIPS-199 ? Evaluate threats and vulnerabilities of each system and ensure proper safeguards are in place to protect the environment ? Utilize processes within the Security Assessment and Authorization environment such as system security categorization, development of security and contingency plans, security testing and evaluation, system accreditation and continuous monitoring. ? Supporting client of creating Risk Based Decisions or Risk Acceptance as part of POA&M remediation. ? Supporting Client and Cloud Service Providers in FedRAMP ATO processes. IT Security Analyst Abiatech Solutions March 2014 to July 2016 Duties included: ? Worked with Assessment and Authorization team; performed risk assessment; updated System Security Plan (SSP), contingency plan (CP), Privacy Impact Assessment (PIA), and Plan of Actions and Milestones (POA&M) ? Assess the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system(s) ? Supporting the VA with mapping evidence for controls and uploading in the GRC. ? Reviewing Risk assessment in GRC to ensure the process is completed and ensure document is updated and uploaded under the applicable entity in GRC ? Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), and E-Authentication with business owners and selected stakeholders. ? Performed comprehensive Security Control Assessment (SCA) and prepare report on management, operational and technical security controls for audited applications and information systems. ? Reviewed audit logs and provide documentation guidelines to business process owners and management ? Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Miles tones (POA&M), Authorization letter Review Technical Security Controls and provided implementation responses as to if/how the Systems are currently meeting the requirements/memorandum (ATO). Education Bachelor of Science University of Buea Skills Active Directory, access Certifications/Licenses CompTIA Security+ in progress, Certified Authorization Professional (CAP) in progress.Scrum Master Certified, Cloud Security Alliance Certified. Present Additional Information Skills Summary ? Expertise in all applicable National Institute of Standards and Technology Special Publication (NIST SP 800 Series) documentation: Performed assessments, POAM remediation, and document creation using NIST SP 800-53 Rev 4. ? Experienced in the developing, Reviewing and updating Security documents such as System Security Plans (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, and Configuration Management Plans, System Security Checklists, Privacy Impact Assessments, POA&M, ? Familiar with VMware and other Virtual Machine Applications ? Good communication and writing skills ? Experienced working with All NIST SP 800 series and FIPS documents ? Experienced with vulnerability Scanning tools such as NESSUS, Web Inspect and Nexpose ? Experienced in Vulnerability Scanning analyzing results / Report from Scanning ? Experienced with developing and updating SOP and Risk Acceptance ? Experienced in Network monitoring and reviewing logs ? Experience with Payment card industry Data security standards (PCIDSS) and the ISO 27001 Series. ? Experienced with Ticketing System- Validating tickets ? Experienced in the six steps of the Risk management framework such as categorization, selection, and implementation, Assessment, Authorization and Monitoring. ? Experienced with Incident Response plan and update.p Technical Skills: ? Software: MS Office (Word, Excel, Outlook, Access, PowerPoint) ? Vulnerability & Penetration Testing Tools; NESSUS, Web Inspect, Nexpose ? SIEM tools such as Splunk and Tenable Security Center. ? Working knowledge of ticketing system such as Remedy BMC and ServiceNow. ? Good Networking Knowledge: LANs, WANs, VPNs, Routers, Firewalls, TCP/IP ? Network Monitoring tools such as snort IDS/IPS, Cisco IOS Firewalls

Name: Crystal Decker

Email: valerie10@example.org

Phone: +1-704-289-5303x38464