Cyber Security Jr. Analyst Cyber Security Jr. Analyst Cyber Security Jr. Analyst - KForce To make valued contributions in a challenging position that maximizes my skills, strong work ethic, and education to obtain a bottom-line improvement in support of the company vision. Work Experience Cyber Security Jr. Analyst KForce - Alexandria, VA September 2018 to Present Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. Performed risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Monitored controls post authorization to ensure constant compliance with the security requirements IT Support Specialist United States Army National Guard - Washington, DC March 2017 to Present Network and System Administration Assist with solving technical issues with the system Keep network infrastructure up-to-date and secured. Write and maintain network security policies and monitor compliance. Identify and recommend needed and optimal infrastructure improvements. Troubleshoot various network issues affect solutions and collaborate with staff and outside vendors to resolve complex problems. Analyzed software hardware and network systems for various transmission systems. Configured and installed routers switches and wireless controllers. Evaluated complex computer systems to assess vulnerability and risk. Worked with outside vendors and teams to develop voice and data wiring infrastructure. Maintained all network documentation for hardware configuration and licensing. Set up user accounts and user permissions, approve accounts and user roles Reset passwords, lockouts, etc. Input user account information under respective contracts Information Assurance Analyst EZ Shield, INC - Baltimore, MD February 2016 to April 2018 Used technologies Nessus, WebInspect, DbProtect Operated Systems Microsoft Windows (Win7/10, 2008, 2012 Server) Specialties Skills NIST, FISMA, Security Analyst, Application Support, Problem Solving, Strong Analytical & Collaboration, Technical Support & Customer Service Experience in executing Step 4 (Security Assessment) of the NIST Risk Management Framework (RMF) Help in updating IT security policies, procedures, standards and guidelines according to department and federal requirements. Participate in client interviews to determine the security posture of the ystem. Supported the Information Assurance (IA) team to conduct risk assessments, documentation for Security Control Assessment, vulnerability testing and scanning. Prepare and submit Security Assessment Plan (SAP) for approval. Monitor controls post authorization to ensure continuous compliance with the security requirements. Supported the Security Assessment and Authorization process of the clients' systems as a Security Analyst Prepare and update the Security Assessment Report (SAR) Support the Security Assessment and Authorization process of clients' systems to obtain ATO. Interpret and evaluate implementations of NIST 800-53 rev 4 security controls. Document findings within Requirements Traceability Matrixes (RTMs) and Security Assessment Reports (SARs). Review all security controls and provide implementation responses to meet requirements. Validate items uploaded into POA&M in support of closed findings. Meet with ISSOs and other stakeholders to discuss findings and process of remediation to ensure weaknesses identified are corrected to an acceptable risk level. Prepare Authorization to Operate (ATO) packages to be disseminated to Authorizing Official for system enrolment, operation and maintenance Jr. IT Security Analyst Trusant Technologies, LLC July 2014 to February 2016 Executed Security Control Assessments Interpreted and evaluated implementations of NIST 800-53 rev 4 security controls Documented Security Assessment Reports (SARs). Conducted Vulnerability scans and compliance using Nessus and Web Inspect. Executed Authorization to Operate (ATO) activities and delivered supporting documentation within aggressive timelines. Assessed systems of varying scope and complexity that comprised of various technologies. Worked on multiple assessments simultaneously. Attended client meetings as necessary. Provided weekly status reports. Update IT security policies, procedures, standards and guidelines according to department and federal requirements using steps of the SA&A (Security, Assessment and Authorization) Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus Vulnerability Scanner to detect potential risks on a single or multiple asset across the company network Veterans Affairs Contract Proposal -Directly assisted Chief of Operations with RFP -Coordinated and corresponded w/ subcontractors via email/phone -Sat in on conference calls w/ western coast partners for contract status updates -Constructed an imperative section of the proposal in the Past Performance section to comply with Veteran Affairs RFP-SOW -Constructed/Distributed PPTs and memos to partners/subcontractors Communications Committee -Attended weekly meetings to strategize with communications team -Managed social networking platform for company Experience working with online ticketing applications/systems (Kayako)(Remedy) ? Activating User Accounts ? Delegating User Roles ? User Permissions ? Phone tickets Software Scouting ? Attended web seminars ? Attended live seminars for software briefings ? Corresponded with software reps and engineers Data Management experience: - Managing inventory ? Excel Spreadsheets/Access ? File Sharing (Sharepoint/GoogleDrive) ? Distributed company Item Receipts/Equipment Agreements/Usage Policies Retrieving company equipment due to usage violations or employment termination Education Masters in Science in Information Systems George Washington University 2020 Information Technology Specialist United States Army Cyber Center of Excellence 2017 Bachelors of Science in Computer Science Simon Fraser University 2014 St. Marys Ryken High School May 2010 Advanced Cisco Unified Communication Management United States Army Cyber Center of Excellence - Fort Gordon, GA Skills Cyber Security, Information Security, Comptia, Information Assurance, It Security, Cybersecurity, Nist, Network Security Military Service Branch: United States Army Rank: E3 Certifications/Licenses CompTIA Security+ January 2019 to January 2023 Comptia Security +

Name: Samantha Pittman

Email: nealmichael@example.net

Phone: 205-816-3876x8145