Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Middle Tennessee Membership Electric Corporation Indianapolis, IN Work Experience Cyber Security Analyst Middle Tennessee Membership Electric Corporation October 2017 to Present   Act as a Subject Matter Expert in the discovery and investigation of critical security vulnerabilities of identified gaps and make recommendations to IT team and oversee implementation   Gather and documentation technical information in support of audits and drive remediation efforts.   Use Tenable Security Center (Nessus) to perform vulnerability scans and provide guidance to patch teams on remediation plans and process.   Perform Risk Assessment on third parties/Vendors to limit exposure of Corporate network.   Routinely perform Email and domain analysis and scans using Virus total Develop a Business Continuity Plan and relationship with outsourced vendors. Developed, reviewed and updated Information Security System Policies, System Security Plan (SSP), and Security baselines in accordance with NIST, FISMA, III A-130, NIST SP 800-18 and industry best security practices.   Perform Users' security awareness and training against social engineering using Knowb4.   Used Rapid7InsightIVR for incident management and SIEM tool   Provide support to internal and external audit teams in gathering evidence to validate PCI compliance.   Endpoint Protection and Data Loss Prevention implementations and Incident Response Plan and Procedures.   Create policies, procedures, processes, memos, work flow diagrams & Reliability Standard Audit Worksheets.   Use NERC-CIP compliance standards to secure SCADA environment.   Developed security control baseline and tested plan used to assess and implement security controls. Cyber Security Analyst Defense Logistics Agency - Philadelphia, PA March 2015 to October 2017 Develop and update System Security Plan (SSP), Privacy Impact Analysis (PIA), System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M)   Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB, NIST SP 800-18 and industry best security practices.   Risk Management Framework (RMF) to do Security control Assessment Using NIST 800-37 as a guide, assessments and Continuous Monitoring   Perform PCI compliance Audits with external auditor on card holder environment.   Performed vulnerability scan and continuous

monitoring after authorization (ATO) to ensure continues compliance with the security requirement.

  Put together Authorization Packages (SSP, POA&M and SAR) for Information systems to the Authorization Officer.   Conduct and evaluate IT/OT security updates on over 128 devices such as firmware, WSUS, Anti-Virus, logging, training, incident response, & recovery operations.   Scan emails against Phishing vulnerabilities using Virustotal Cyber Security Analyst ADP - Chicago, IL April 2014 to March 2015 Identified trends and root causes of system failures or vulnerabilities using NESSUS Vulnerability Scanner, Nmap to scan ports, weak configuration and missing patches Conducted a review of the plan of action and milestone (POA&M) process to ensure corrective actions and timely mitigation of the vulnerabilities Maintain and support of the Oracle E-Business Suite (EBS), PeopleSoft application   Supported the Information System Security Officer (ISSO) and collaborated with the system's Information System Owner (ISO)c   Reviewed and updated the system security plan for the security controls put in place or planned   Assisted the ISSO in the implementation phase of RMF to document security controls in system security plan (SSP) and contingency plan (CP).   Collected and validate artifacts from the system owner to support quality information system audit and review.   Performed Security control assessment (SCA) using NIST 800-53Arev1 per NIST, FISMA standard and guidelines. Senior Oracle Database Administrator Cigna - Minneapolis, MN June 2010 to March 2014   Experience designing and maintaining Oracle 10g, 11g and 12c relational databases.   Convert non - container database to pluggable in Container databases (12c). Patched the Oracle E-Business Suite (EBS) and PeopleSoft application   Apply upgrade patches, maintenance and interim patches on production and non-production databases.   Implemented TDE and advance security to encrypt mask secure sensitive data with the use DB Vault Education Master's in Cyber Security Engineering in Cyber Security Engineering University of Maryland Links https://www.linkedin.com/in/bless-mbah-499642181

Name: Bailey Hudson

Email: dgarcia@example.com

Phone: 001-276-488-5776x48122