Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - SecureStrux College Park, MD Work Experience Senior IT Security Analyst SecureStrux - Arlington, VA May 2016 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. * (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 * Conduct Self-Annual Assessment based on NIST SP 800-53A * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burp Suite and DbProtect scans for possible remediation. * Assess systems of varying scope and complexity and comprised of various technologies. * Create standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages * Provide weekly status reports on ongoing tasks and deliverables IT Security Analyst MindPoint Group - Springfield, VA June 2013 to May 2016 * Assisted in conducting cloud system assessments * Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). * Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements * (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). * Worked with client in safeguarding CUIs by performing the necessary assessments which primarily deals with 14 control families. * Support Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification

and Accreditation, and Computer Network Defense. * 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 Junior IT Security Analyst Resolution IT consulting group - Woodbridge, VA February 2012 to June 2013 * 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). Alarm Monitor/ Entry cybersecurity analyst Admiral Security - Washington, DC December 2009 to February 2012 * Experience reviewing and interpreting Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burp suite and DbProtect scans * Assisted the SOC team in documenting and reporting vulnerabilities by utilizing tools such as Splunk and SNORT. * Developed security reports and presented to supervisors as needed. * Participated in sensitive briefings on security issues and classified information. * Recommended improvements in security systems and procedures. Designed security policies, alarm response protocols and access card guidelines. * Implemented video surveillance, motion detection and closed-circuit television systems to aid in monitoring the premises. * Log alarms in the security log. * Authenticate all openings and closing of SCIFs' and open storage areas, using the open/close Sop's. Log all entries in on the security log form. Inventory and account for all equipment prior to relieving the off-going shift issue all equipment on a hand receipt. * Monitor all post rotations; ensure stationary posts are properly manned at all

times during the rotations. * Conduct hourly radio status checks with all post and patrols, Report all building and personnel emergencies on and around the facility, and ensure building security during evacuations. Notify the proper authorities using the emergency notification roster; Ensure each post-shift change is completed; the site manager or shift leader will be notified of all discrepancies prior to relieving. * Technical: Monitor/operate an integrated, state of the art access control, Intrusion, alarm, closed circuit, television (CCTV) system. * Monitor/operate an integrated, state of the art access control, Intrusion biometric identification system. Education Associate in Criminal Justice in Criminal Justice Bowie State University - Bowie, MD Skills NESSUS (8 years), NIST (6 years), SNORT (2 years), SPLUNK (2 years), RISK MANAGEMENT, Cissp, Information Security, Cyber Security, It Security, security, access, powerpoint Additional Information Summary of skills: Risk Management Framework   NIST 800-53   Nessus   WebInspect   Splunk   DbProtect SNORT

Name: Peggy Johnson

Email: mercadomiguel@example.org

Phone: 795.673.9724x3771