

IT Security Analyst IT Security Analyst IT Security Analyst - The Nigbel Group Woodbridge, VA

Well-informed specialist with diverse experience in advanced technology. Firm background as an IT Specialist with a smooth transition to excel as an IT Security Analyst. Proficient working independently or collaborating with team members. Work in a timely manner of executing deliverables to senior executives in an organization. Process driven and detail oriented. Excellent written and verbal communication skills

Work Experience IT Security Analyst The Nigbel Group May 2013 to Present

Provided support and maintenance of the Critical Infrastructures systems in addition to other systems supported by the BVTI team. Served as a technical lead professional for assigned functional areas and assisted subject matter experts with ensuring data integrity, testing of system changes, report writing and analyzing data flows for process improvement opportunities.

Conduct Pre-assessment and Post-assessment activities for the assigned systems

Developed System Assessment and Authorization (SA &A) packages for compliance with NIST guidance, including System Security Plans, System Categorization documents using FIPS 199, Risk Assessment, POA&M, Contingency Plans, and Private Impact Assessments (PIA).

Review Information System Security Policies and Procedures, System Security Plans (SSPs), and Security baselines in accordance with NIST, FISMA and Industry best security practices.

Support the PM during the initial SA&A kick-off meetings to explain the C&A process to the stakeholders unfamiliar with the process.

Assess Security Controls through document review, interview, and test procedures to ensure compliance with FISMA, and NIST SP 800-53A Rev 1.

Schedule, track and manage the monthly and quarterly POA&M review process.

Responsible for performing Network scans using Nessus Tenable Security tools (NESSUS) to identify network vulnerability and submit technical reports detailing the vulnerabilities, risk, and remediation action.

Utilize the NIST 800-53 Rev 3 and NIST 800-53 Rev 4 to conduct security control testing, with results documented in a Security Requirements Traceability Matrix (SRTM) to determine each system in compliance with Federal Security Standards.

Maintained and supported a variety of reports or queries utilizing appropriate reporting tools. Assisted in development of standard reports for ongoing customer needs. Helped maintain data integrity in systems by running queries and analyzing data.

Ability to

work in a dynamic, responsive, and collaborative environment, and dedicated to the success to customers against advanced, persistent threats. Apply FISMA methodology to include NIST 800-37 to build a risk management framework to deploy accurate and up-to-date security documentation (PIA, CP, CMP, DRP, SSP, RA, RMR) and used NIST 800-53 controls for testing and preparing POAM activities for risk mitigation and continuous monitoring. Education BSc. in Computer Science University Of Nigeria Awards Experience in handling various aspects of Information Systems Security Authorization and Continuous Monitoring process based on the Special Publications by NIST (800-60 & FIPS 199, OMB circular A130 App III, 800-53 Rev 4 & FIPS 200, 800-53a Rev.4, 800-137, 800-37 Rev 1, 800-30) Proficient in developing and working with System Security Plan (SSP), Plan of Action & Milestone (POAM), Security Assessment Plan (SAP), Security Testing & Evaluation (ST& E), Security Assessment Report (SAR) Certifications/Licenses Certified Authorization Professional (CAP) (CAP) Certified Authorization Professional Comptia Security + - In progress

Name: Linda Carson

Email: catherinemendez@example.org

Phone: (697)538-1631