Sr. Security Analyst Sr. Security Analyst Sr. Security Analyst - Transportation Security Administration Houston, TX Work Experience Sr. Security Analyst Transportation Security Administration October 2012 to Present * Determine baseline security configuration standards for operating systems, networking, encryption, data security, data classification, and identity and access management (IAM) assuring architectures meet security best practices * Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment * Develop security standards, procedures, strategy plans, and roadmaps based on sound enterprise architecture practices. * Implement specific cybersecurity countermeasures for systems and/or applications. * Perform security reviews, identify gaps in security architecture, and develop a security risk management plan * Conduct full lifecycle Certification & Accreditation (C&A) tasks utilizing NIST guidance to assure FISMA compliance for TSA systems * Implement security measures across all OSI layers to include firewalls, gateways, IDS, HIPS and network routers. * Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative. * Demonstrate effective networking skills as it relates to cybersecurity and TCP/IP implementation enterprise wide. * Provide cybersecurity recommendations to leadership based on industry best practices (e.g., ISO, OWASP, NIST, SANS) * Provide security support and network assessments for Azure cloud implementations across the TSA enterprise Sr. Security Analyst Department of Labor - Washington, DC September 2011 to October 2012 * Conducted full system security control assessment, testing and well as integration support for the department * Assist in developing and implementing information security compliance policies, standards and procedures * Develop security vulnerability test plans and perform security tests utilizing various industry standard tools * Support operational readiness reviews and help with enforcing security requirements within projects and the Software Development Lifecycle (SDLC) * Provide cybersecurity recommendations to leadership based on industry best practices (e.g., ISO, OWASP, NIST, SANS) * Demonstrate effective networking skills as it relates to cybersecurity and TCP/IP implementation enterprise wide. * Assisted with the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements as well as conduct privacy impact assessments * Correlate multiple data sources to identify vulnerabilities, make recommendations and work with system owners to expedite remediation * Assisted with security planning and compliance guidance under FISMA and FedRAMP for cloud implementation. Security Consultant AUSGAR Technologies September 2008 to September 2011 * Participated in the design and oversight of vulnerability assessments and security audits * Served as Information Security subject matter expert / liaison to various client business groups * Assess technical security requirements using assessment techniques, tools and methodologies * Network engineering tasks to include system design, system build as well as assure the secure development of Windows systems and network appliances * Developed and maintained documentation such as Risk Assessments, Privacy Impact Assessments, System Categorization, System Security Plans, Contingency Plan development, ST&E development and all other DIACAP/NIST C&A documentation for FISMA compliance * Works with manager to maintains an up-to-date understanding of industry best practices or frameworks such NIST CSF, ISO, HIPAA, PCI, * Conducted vulnerability assessments at various client engagements during all phases of the system development life cycle (SDLC) Principal IT Security Consultant General Dynamics May 2003 to September 2008 * Provided security engineering and security Certification & Accreditation support for DITSCAP/DIACAP/NIST efforts to bring organizations into FISMA compliance * Assist with Business Development efforts and Request for Proposal (RFP) responses * Work with the business and management to analyze current and emerging security risks and recommends security solutions and changes * Led Security Risk Assessments of complex technical and business environments and Recommend security enhancements to systems and network components * Conducted vulnerability assessments as well as PCI-DSS assessments at various client engagements Sr. Systems Security Engineer National Aeronautics Space Administration (NASA) - Washington, DC June 2000 to February 2005 Sr. Security Engineering Consultant Signal Solutions May 2002 to May 2003 * Developed policies, standards and procedures to comply with federal and state rules and regulations. Regulations integrated into project include PCI, HIPAA, DITSCAP/DIACAP * Generated security management plans as well as trusted facilities manuals to enhance the secure posture of Army systems * Conducted vulnerability assessments at various client engagements * Analyzed and defined the business and security requirements of multi-tiered information systems * Performed security risk assessments of Technical and business environments and Recommended security enhancements to systems and network components * Perform security test and evaluation and generate ST&E documentation Sr. Network Engineer CSSI, Inc - Washington, DC January 1999 to June 2000 Network Administrator Arcadia University - Glenside, PA December 1997 to January 1999 Education Bachelor of Science Wesley College - Dover, DE 1997 Skills Security, Disaster recovery, Information security, Nessus, Nist, Nmap, Pci, Fisma, Incident response, Network administration, Hippa, Gap analysis, Configuration management, Sarbanes-oxley, Sarbanes-oxley act, Contingency planning, Audits, Lan, Active Directory, access, Cisco, training Additional Information Security Clearance Secret Total Years IT Experience 15+ Years Supporting Security Engineering, Information Assurance, Cybersecurity 15+ Relevant/Special Experience, Training, or Qualifications Project Management Institute (PMI) Member Infraguard Member Proficient with Microsoft Office applications Experienced Public Speaker Member of various tech councils Skill Summery Overview: An Information Assurance and Cybersecurity leader with an extensive background driving proactive security initiatives in a variety of organizations while participating in the development of progressive security architecture and policy framework solutions, which directly support business goals and mission objectives. Areas of Expertise: Audits and Assessments, Compliance Verification, Security Gap Analysis, Security Incident Response, Information Security Management, LAN/System/Network administration, Configuration Management, Contingency Planning, Disaster Recovery, et al. Tools & Regulations: Nessus, AppScan, WebInspect, HP Fortify, NMAP, Retina, CSAM, Xacta, CSET, HIPPA, HITRUST, FISMA, DIACAP, PCI-DSS, NIST-800, Sarbanes-Oxley Act, Cybersecurity Framework (CSF)

Name: Michael Wilson

Email: david65@example.org

Phone: (441)222-6525x13073