Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Vangarde LLc Centerville, UT Work Experience Cyber Security Analyst Vangarde LLc December 2016 to Present Responsible for supporting multiple PIT systems and Information System Security Managers (ISSM). Responsibilities as a Information Systems Security Officer (ISSO) include ensuring delivery of information systems that meet all security standards in accordance with government guidelines and the NIST Risk Management Framework (RMF) process. Creating or updating program artifacts. Documenting comprehensive configuration management plans for software, hardware, firmware, and peripherals for Information Technology (IT) systems. Documenting review and audit results for IT system configurations. Documenting assessments of cybersecurity risks associated with information systems according to published policies, standards, and procedures. Collaborating in a diverse technical team environment. Support Information security sustainment via RMF continuous monitoring activities. IT Security Spec IV Federated IT June 2016 to September 2016 Responsible for supporting nationwide Cyber Security policies and activities of the US Department of labor (DOL) IT networks, systems and applications including Vulnerability Management (Host/Network Nessus scanner), Incident Reporting, Mitigation, and Continuous Monitoring. Responsibilities include technical oversight, coordinate and report on all security incidents. Review, analyze, test and authorize network/software/host change requests that have security implications to the production environment. Monitor and manage security IDS and IPS systems for malicious traffic and intrusions. Interpret requirements and guidance to ensure customer systems, applications, and operations adhere to policy and best practices. Real-time Cyber Security Analyst OnPoint Consulting May 2013 to February 2016 Responsible for supporting all aspects of the National Nuclear Security Administration Information assurance Response Center. Responsibilities include monitoring, collecting and analyzing daily threat event information. Provide operations support for a 24/7 operational environment comprising of networks, enclaves, and systems. Provide threat incident handling, reports and analysis for daily reports and presentations. Interprets, analyzes, and reports all events and anomalies in accordance with Computer Network directives, including initiating, responding, and reporting discovered events. Coordinate and distribute directives, vulnerability, and threat advisories to on-site personnel and customers. Provide daily summary reports of network events and activities for metric reporting. Information Systems Security Engineer L-3 Stratis July 2010 to April 2013 Responsible for supporting all aspects of the DISA Global NetOps Support Center (GNSC) Net Assurance (NA) operations including dynamic Information Assurance (IA) operational support. Responsibilities comprise of providing operational and technical analysis/direction for network information security issues. Monitor DOD networks for malicious activity utilizing DISA IA tools. Investigate, report and coordinate suspicious activity with DOD customers. Provide computer incident handling, reporting and analysis for daily reports and presentations, ensuring accuracy and compliance with DoD standards, Joint Task Force Global Network Operations and DISA security policy, doctrine and regulations. Provide risk management, security policy enforcement and reporting, assuring compliance with established security procedures. Creating & reporting events/incidents into Remedy and Joint CERT Database (JCD) ticketing system. SATCOM Equipment Specialist U.S. Air Force Engineering and Technical Services April 2009 to April 2010 OJT) on data networks and provide technical support on complex and sophisticated deployable Satellite Communication System / IP Network equipment. Responsibilities include training user and maintenance community. Provide corrections to design deficiencies through evaluation of operational capability of systems /equipment; review of performance data against standards. Provide network communications and network services to include planning, analysis, design, development, testing, quality assurance, information assurance, configuration, implementation, integration, maintenance and /or management of network systems used for the transmission of secure / non-secure information in voice, data, and /or video formats. System/Test Engineer Raytheon November 2006 to November 2008 Support the development of system(s) requirements and architecture of the GPS OCX program from the beginning phases of a project through sell off and final customer acceptance. Responsibilities include correction and update of system design documents, contribute to, or make, presentations, attend meetings and reviews. Provide Analysis and recommend appropriate configuration, equipment and software changes to satisfy customer, design change requests. Represent the SE organization in providing solutions to technical issues. As a Test Engineer responsible for developing test & verification plan documentation for the NPOESS program. Participate in engineering requirement reviews, design and test readiness reviews. Coordinate with multidisciplinary engineering teams and conduct technical documentation peer reviews. Ensure successful verification and validation of test requirements; verify compliance of established test plans, requirement and test procedures. Education Bachelor of Science in Computer Info System Columbia College AAS in Advance in electronics Colorado Aero Tech Institute Skills Dns, Disaster recovery, Ids, Ips, Nessus, Cyber Security, Information Security, Nist, Siem, It Security, Network Security, Comptia, Linux Military Service Branch: United States Army Rank: E-4 Certifications/Licenses Security plus (+) CE CompTIA (COMP001021141242) September 2016 to September 2022 (CEH) Certified Ethical Hacker (EC-Council #ECC943144) August 2010 to Present Additional Information SUMMARY OF SKILLS: Experience in aerospace programs, from conceptual design through product development, integration, and testing. Experience in requirements development, system development lifecycle and systems engineering processes. Diverse experience in Cybersecurity environments and tools. Cybersecurity experience with realtime monitoring (SOC) through analysis and reporting. Cyber tool knowledge and experience using SIEMs Arcsight, Trustwave, Qradar. Ticket management and change request process knowledge using Remedy tool. Knowledge of TCP/IP Networking, DNS, Disaster Recovery, Host/Network Nessus scanner, security concepts (IDS/IPS). DoD 'Secret' clearance (May 2019).

Name: Bobby Torres

Email: sara54@example.org

Phone: (521)872-0058x235