

IT Security Analyst IT Security Analyst IT Security Analyst - G2, Inc Washington, DC Work Experience IT Security Analyst G2, Inc - Annapolis Junction, MD November 2016 to Present *

- Assisted in conducting cloud system assessments
- * Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements
- * 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 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 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 Infotek Corporation - Columbia, MD April 2015 to November 2016

- * supports the Security Assessment and Authorization process of the clients' systems as a technical Security Analyst
- * 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.
- * Helped with updating IT security policies, procedures, standards, and guidelines per the respective department and federal requirements.
- * Performed risk assessments

to identify the risk level associated with the findings * (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 * Reviewed artifacts regarding Plans of Action and Milestones (POA&M) created by ISSO before closing * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans for possible remediation. * Assess systems of varying scope and complexity and comprised of various technologies. Security Specialist/ Entry level information security analyst GAP Solutions - Rockville, MD December 2013 to April 2015 * Provide weekly status reports on ongoing tasks and deliverables * Provide trend analysis and data reports associated with tracking case workload and cycle time associated with all work performed * Other job duties assigned * Reviews requests for security clearances, evaluating the sensitivity classification of the position by applying need-to-know principles and pertinent security guidelines * Conduct facility clearance surveys for contractors entering the NISP * Conduct recurring security vulnerability assessments, physical security inspections of contractor plants and facilities performing work for the government involving the storage and/or production of sensitive arms, ammunition and explosives. * Conduct security vulnerability assessments of cleared industrial facilities performing on classified contracts for the U.S. * Provides security oversight and assistance to assigned contractor facilities for information systems (IS) processing classified information. IT Intern/ Junior security analyst WMATA/SRML - Washington, DC May 2011 to December 2013 * Policy writing and understanding of NIST publication * Assisted in updating IT security policies, procedures, and standards according to NIST * Worked in SOC environment in order to conduct scans and identify vulnerabilities * Worked with network security (network administrator policies, procedures, firewalls, etc.) * Assisted in technology management * Troubleshoot hardware and software * Assisted cyber team in conducting assessments and reports of systems * Utilized Nessus Education MSA in Academy Prince George's Community College - Washington, DC Skills Nessus, Nist, Ms office, Sap, Risk management, Sar

Name: Brittany Moody

Email: burnettseth@example.org

Phone: 933-683-7159x768