

IT Security Analyst IT Security Analyst IT Security Analyst - InfoTek Corporation Baltimore, MD I have several years of experience in the information assurance and information security discipline. I am knowledgeable of the Risk Management Framework (RMF) and how it relates to the System Development Lifecycle (SDLC), and Cyber Security Framework (CSF). I am skilled in the execution of Security Assessment & Authorization (SA&A), Plan of Action & Milestone (POA&M) activities, scheduling, tracking, and providing project status updates to management. I developed, maintained, and updated SA&A-related documentation such as the Security Assessment Report (SAR), System Security Plan (SSP), and Risk Assessment (RA).

Work Experience IT Security Analyst InfoTek Corporation June 2014 to Present

- Experience in cloud system assessments, primarily with AWS (Amazon Web Services) by utilizing FedRAMP and NIST guidelines
- Experience in executing Step 4 (Security Assessment) of the NIST Risk Management Framework (RMF).
- Experience in developing and disseminating Security Assessment Plans.
- Experience in interpreting and evaluating implementations of NIST 800-53 rev 4 security controls.
- Documenting findings within Requirements Traceability Matrixes (RTMs) and Security Assessment Reports (SARs).
- Experience reviewing and interpreting Nessus Vulnerability and Compliance scans, WebInspect scans, and DbProtect scans
- Ability to execute Security Assessments and develop and deliver supporting documentation within aggressive timelines.
- Assessing systems of varying scope and complexity and comprised of various technologies.
- Work on multiple assessments simultaneously.

Junior Information Security Specialist Kaizen Approach, Inc April 2012 to June 2014

Provide trend analysis and data reports associated with tracking case workload and cycle time associated with all work performed.

- ? Other Job duties as 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. Junior SOC Analyst Applied Integrated Technologies December 2010 to April 2012 Responsible for monitoring and troubleshooting the electronic security systems (ESS) Supervised 4 Operators on each shift including myself. Monitored multiple accounts across agencies, and use open sources tools to determine potential threats for the network. Used remedy to monitored and updated incoming/assign tickets. Provide support to agency users. Use remedy to monitor and update incoming/assign tickets. Responsible for working in a 24x7 Security Operation Center (SOC) environment Utilized SNORT for packet logging and traffic analysis Proficient with scanning tools such as Nessus Receive and transmit routine and emergency call in the Security Operations Center, administer routine and emergency call assignments and operations.

Provide armed and uniformed security, force protection, and law enforcement functions. Helpdesk/Junior Information Security Analyst Resolution IT consulting Group May 2009 to December 2010 Assisted in technology management Troubleshoot hardware and software Policy writing and understanding of NIST publication Assisted in Updating IT security policies, procedures and standards according to NIST Worked in a SOC environment in order to conduct scans and identify vulnerabilities Worked with network security (network administrator policies and procedures, firewalls, etc. Installing New Local and Network Printers and configurations Proactively and reactively research the root cause of and provide solutions or known work-arounds for Problems in the Enterprise environment. Assisted cyber team in conducting Assessments and Reports of systems Education SSP in SAR NIST

Name: Julian Moore Jr.

Email: jeremymay@example.net

Phone: 8997195423