

JUNIOR SECURITY ANALYST JUNIOR SECURITY ANALYST JUNIOR SECURITY ANALYST, PJ
PROFESSIONAL IT SERVICES - Security Categorization Greenbelt, MD Experienced Junior
Security Analyst with a demonstrated history of working in the Information Technology &
Cybersecurity services industry. Skilled in Information Systems Security, Cybersecurity policies,
Risk Management Framework, NIST publication, Office 365 (Excel, Microsoft Teams, Word,
SharePoint, Note, PPT), Nessus, Windows Operating System. Seeking to leverage my skills and
knowledge and help organizations reach their maximum potential. Work Experience JUNIOR
SECURITY ANALYST PJ PROFESSIONAL IT SERVICES January 2016 to Present Conducted
security assessments on OS and network based on the NIST Risk Management Framework to
identify security weaknesses. Support systems through all steps of RMF to achieve and or
maintain authorities. Provided guidance of needed evidence to satisfy security controls and
documenting findings of assessments. Developed Security Assessment Plan (SAP) to conduct
security assessment. Coordinated and schedule kick-off meetings for the A&A process for system.

Reviewed the FIPS 199 Security Categorization of the overall impact level of systems.
Scheduled interview meetings with control owners and other stakeholders. Reviewed System
Security Plan (SSP), Configuration Management Plan (CMP), Contingency Plan (CP) and other
security policy documentation. Tested security control implementations in accordance with control
guidance documented in NIST SP 800-53 rev4. Develop Security Assessment Reports (SAR) to
support accreditation package. Work with system engineers to assemble accreditation packages,
including SSP, SAR, POA&Ms, etc. Ensured information systems security documentation
templates (e.g. System Boundary development, System Security Plan (SSP), Contingency Plan,
Contingency Plan Test, Business Impact Analysis,) remain up to date based on perpetually
changing NIST Examined artifacts and review control implementation status with control
requirements. Uploaded and updated POA&Ms, SARs, SSPs, SOPs for remediation. Tier 1
Technical Support CAPITAL DIABETES AND INTERNAL MEDICINE January 2015 to January 2016
1 SUPPORT, CAPITAL DIABETES & INTERNAL MEDICINE Responded to requests for technical
assistance via phone, electronic communications, and in person. Installed and set up equipment

and hardware/software for new and existing employees Monitored the remote monitoring and management system alerts and notifications and respond accordingly. Researched and resolve technical issues involving Microsoft's core business applications and operating systems using available information resources. Communicated with customers by keeping them informed of incident progress, notifying them of impending changes, and agreed outages. Implemented issue resolution and/or advise user on appropriate action Followed standard help desk procedures

Logged all help desk interactions Redirected problems to tier 2 and tier 3 level support as required

Assisted senior IT staff as needed IT OPERATIONS SUPPORT AMERICAN AIRLINES November 2013 to January 2015 Responded to Flight Attendants general questions in person and by phone

Installed and configures local and network-based printers Provided Tablet support at the Crew Service Centers Assisted in the coordination of Flight Attendant parking and Crew IDs Ordered supplies and maintains the e-board in the crew rooms Assisted the Duty Managers with all aspects of Flight Service IT operation Ensured office and crew room computers and equipment are in working condition Troubleshooted and collaborate with other departments

Education BACHELOR OF SCIENCE VIRGINIA STATE UNIVERSITY - Petersburg, VA December 2011 Skills Nist, Fisma, Scanning, Problem-solving, Presentation skills Links <http://www.linkedin.com/in/caseypridgen>

Certifications/Licenses Certified Ethical Hacker (CEH) Additional Information SKILLS Excellent communication, collaboration, and presentation skills. Proven results-oriented problem-solving abilities. Ability to work in a dynamic team-oriented environment, demonstrate teamwork and initiative, and function productively in a dynamic work environment Ability to adapt in a fast paced and time sensitive environment Knowledge of NIST/FISMA/requirements and policies.

Experienced in Vulnerability Scanning. Ability to communicate orally and through writing. Ability to conduct periodic assessments of systems to ensure compliance with security requirements.

Name: Tonya Johnson

Email: patriciafarmer@example.org

Phone: +1-811-200-2006x4871