Network Security Analyst/SOC Analyst Network Security Analyst/SOC Analyst Network Security Analyst/SOC Analyst Bowie, MD With continuous monitoring, I can interpret and prioritize threats using Intrusion Detection/Prevention Systems; Firewalls; Security Incident/Event Management (SIEM). I can recognize potential, successful, and unsuccessful intrusion attempts and compromises through analysis and review of security events, logs and network traffic. I can also document incident findings, analysis steps, and create management level reports. I can proactively monitor and mitigate information security Authorized to work in the US for any employer Work Experience Network Security Analyst/SOC Analyst United States Department of Health and Human Services - Rockville, MD January 2012 to August 2015 Computer Sciences Corporations, Rockville MD January, 2012 - August, 2015 Client: United States Department of Health and Human Services Log analysis, proactive monitoring, mitigation, and response to network and security incidents Analyzed security event data from the network (IDS sensors, firewall traffic). Recommended virus removal steps for infected systems after detection and analysis Rescan mitigated systems for further infections. If none, commission systems back to the network. Continuous monitoring and interpretation of threats through use of intrusion detection systems, firewalls and other boundary protection devices, and any security incident management products deployed. Working knowledge of auditing and compliance under NIST HIPAA guidelines. Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices. Research new and evolving threats and vulnerabilities with potential to impact the monitored environment Use Vulnerability Assessment tools such as Nessus to perform security testing Identify suspicious/malicious activities or codes. Report malicious activity to client locations with recommendations for remediation Worked in a 24x7 Security Operations Center Vulnerability Scanner / IT Security Specialist United States Department of Treasury, Internal Revenue Service - Lanham, MD February 2007 to November 2011 Computer Sciences Corporations, Lanham MD February, 2007 - Nov, 2011 Client: United States Department

of Treasury, Internal Revenue Service Log analysis, proactive monitoring and response to network and security incidents Analyzed security event data from the network (IDS sensors, firewall traffic and routers). Scanned for rogue (unknown) hosts on the network, which includes unauthorized network peripherals such as printers, laptops, PDAs, and taking them of the network for compliance and proper identification Performed adhoc server scans using Nessus and provided compliance to Projects. Develop hardening scripts to conform to IRS's Internal Revenue Manual (IRM) Unix security requirements. Also perform Alpha and Beta test on new security packages Acted as a Subject Matter Expert in resolving and mitigating risks on Unix/Linux servers. Provide SME support for Unix security including server hardening and monitoring Supported Unix SAs with engineering procedures for our Unix environment Use Vulnerability Assessment tools such as Nessus, UPC, and NMAP to perform security testing Identified new malware infections and removed those remotely using admin tools or by identifying the user and guiding them through a removal process. Daily research of existing and new security vulnerabilities including 0-day vulnerabilities. These vulnerabilities are documented and network hosts are patched against these vulnerabilities and threats Supported Federal Information Security Management Act (FISMA) Compliance. Working knowledge of auditing and compliance under IRM and PCI guidelines Generate security reports Provide wireless (802.11x) scanning and removal of unauthorized devices Make enterprise security recommendations and technical evaluation of new solutions Education B.Sc. in Computer Science Bowie State University Skills Network Security (7 years) Certifications/Licenses CompTIA Security+ December 2015 GCIA December 2015 CISSP February 2016 Additional Information KNOWLEDGE AND SKILLS Security Management: Nitro, NetWitness, TipingPoint, FireEye, Snort (BASE Interface), ArcSight, App Detective, IDS Policy Manager, Nmap, Nessus, RSA Security Analytics, Firewall Logs, Remote Administration (VNC, Putty, SSH), CheckPoint Firewall Incident Management: Risk and threat Analysis, Research and assessment, escalation plans and logging (ClearQuest Ticketing system, Remedy), remediation (Tivoli Portal) Software Packages and Programming Languages DbProtect, Tivoli Software, Rational Rose, Microsoft Office Suite, PL/SQL, Unix Shell Scripting, C/C++, Visual Basic, Common Lisp, SQL,

Assembly Language (SAL) SPECIAL SKILLS Great leadership skill. Eager and willing to learn Good Security, Network, and Scripting skills Excellent verbal and written communication skills Great Troubleshooting and Customer Support Service Work efficiently with little or no supervision, and meets deadline Strong Analytical skills and background in Computer Architecture Extensive working knowledge of UNIX and Windows Operating System Environments

Name: Stephanie Johnson

Email: longshelby@example.org

Phone: 532-627-7274x1174