CSIRT Cyber Security Incident Response Analyst 2 CSIRT Cyber Security Incident Response Analyst 2 CSIRT Cyber Security Incident Response Analyst - GCFA, SSCP, Sec+, Net+ Arlington, TX Cyber security professional proficient in host, network, and malware analysis. Highly skilled in research, analysis, and investigation of security incidents and utilization of enterprise security tools. Authorized to work in the US for any employer Work Experience CSIRT Cyber Security Incident Response Analyst 2 Epsilon Data Management - Irving, TX 2017 to Present Perform host, network, and malware analysis and forensics to mitigate and contain security threats. Analyze and research security events and data in enterprise security tools including QRadar SIEM, FireEye IDS/IPS, Symantec DLP, and Symantec Endpoint Protection. Respond to security incidents and follow through from preparation to post-incident activity. Thoroughly document all events during incidents from discovery to resolution in Resilient and CA Service Desk. Create post-incident Event of Interest (EOI), and executive summary reports. Research and recommend improvements to procedures and security tools. Author Standard Operating Procedures (SOP) and procedural runbooks for incident response. Investigate escalated cyber security incidents escalated from tier 1 Security Operations Center (SOC). Senior Desktop Support Analyst Stefanini IT Solution - Irving, TX 2016 to 2017 Administered Active Directory, Exchange Server, Office 365, and file servers. Provided IT support for local and remote tier 2 IT clients at Epsilon Data Management. Provided white-glove VIP and senior leadership technical support. Deployed hardware and software to customer specifications in a diverse enterprise environment. Coordinated imaging and deployment for Windows and MacOS clients. Managed 10,000+ IT assets in asset management system. Train new IT support associates. Provided new hire orientation for technical topics. Manage requests and incidents in CA Service Catalog/Service Desk system. Services provided at Epsilon via Stefanini IT Services Associate Software Engineer JCPenney - Plano, TX 2009 to 2012 Analyzed and gathered requirements for logistics systems and new processes. Developed, upgraded, and maintained distribution center software systems for supply chain, distribution management, and RFID tagging systems for 9 distribution centers and 15 store support centers. Designed test cases in HP Quality Center to enhance and add functionality to logistics systems.

Developed and updated SQL scripts and stored procedures to regularly offload data from production servers to data warehouses providing near real time key performance indicators without affecting production server performance. New hardware selection, prototyping, and implementation for logistics systems processes. Trained and mentored IT associates on logistics systems processes and troubleshooting. Application Support Engineer JCPenney - Plano, TX 2007 to 2009 Supported supply chain, 15 store support centers, and 9 distribution centers nationwide. Administered Red Prairie distribution management software on HP-UX systems. Installed, upgraded, supported, and maintained all aspects of supply chain systems. Researched and identified problems with data consistency and integrity in supply chain systems Oracle databases. Updated codebase to prevent reoccurrence of identified problems. Performed SOX audits to ensure appropriate access levels and disable inactive user accounts. Monitor log files and troubleshoot data inconsistencies and process flaws in warehouse management systems. Trained IT staff at logistics centers to provide first level support of new and existing logistics systems. IT Manager JCPenney - Cedar Hill, TX 2006 to 2007 Managed local IT technicians and Unix Administrators at the Cedar Hill Store Support Center. Identified needs of IT staff and developed personalized training programs to provide career advancement and personal growth. Managed projects and changes, and coordinated installations with local operations management team as well as various IT teams at the corporate office. Managed budget for local IT staff and projects. UNIX Administrator JCPenney - Cedar Hill, TX 2002 to 2006 Administered distribution management software in HP-UX environment, sortation systems, local network, file servers, Oracle and MS SQL database servers, and all IT hardware and software at Lenexa KS and Cedar Hill TX Store Support Centers. Monitored Unix data and log files for errors and corrected data problems to reprocess files as needed. Developed and maintained reporting systems for merchandise sortation equipment utilizing data in MS SQL databases and outputting with ASP and automated email reports. Researched recurring logistic systems problems and performed root cause analysis for data inconsistencies and anomalies impacting proper process flows. Supported all IT related functions for local logistic center users including PC/laptop, laser printers, label printers, RF scanners, and

network equipment. Education Bachelor of Arts in Information Technology Systems Ottawa University - Ottawa, KS December 2004 Associate of Applied Science in Information Technology Tarrant County College - Fort Worth, TX May 2003 Skills Cyber Security, Siem, Information Security Links http://www.linkedin.com/in/andrewschmidttx Certifications/Licenses CompTIA Network+ May 2001 to Present CompTIA Security+ April 2017 to April 2020 (ISC) Systems Security Certified Practitioner (SSCP) February 2018 to February 2021 GIAC Certified Forensic Analyst (GCFA) April 2019 to April 2023

Name: Shawn Greene

Email: carriemorales@example.com

Phone: (310)241-3472