Security Analyst II - Security Operations Center (SOC) Security Analyst II - Security Operations Center (SOC) Security Analyst II - Security Operations Center (SOC) Work Experience Security Analyst II - Security Operations Center (SOC) Alert Logic October 2013 to March 2018 Tuned Web Application Firewall (WAF) policies to ensure maximum availability for applications while providing threat coverage against web-based (http/https) attacks. Work directly with customers to discuss application requirements. Trained less experienced analyst to write policies. Maintain continuous monitoring of a global network intrusion detection system (NIDS). Evaluated attacks against clients to determine if the attacks were successful. Notified clients of successful attacks. Utilized Alert Logic's Log Manager (a log aggregation tool similar to Splunk) to investigate security events. * Created signatures for WAF * Provided support for both data center and cloud systems (AWS, Azure, Rackspace, Peer 1, and others) * Identified website vulnerabilities such as weak authentication or injection vulnerabilities. Government contractor System Integration & Management Inc October 2012 to September 2013 Network Security Officer Supporting the Space and Naval Warfare Command's New Orleans office, primary responsibilities: monitoring Intrusion Detection System and vulnerability scanning. * Held Secret clearance with Single Scope Background Investigation (SSBI) IT Security Analyst The Shaw Group January 2012 to July 2012 Served as technical specialist in the field of IT security. Assisted in the planning, development, implementing and maintaining programs, policies, and procedures, to ensure the confidentiality, integrity, and availability (CIA), of a Fortune 500 company's computer systems. Implemented and administered user accessibility and access controls to computer facilities. Conducted security reviews of critical systems and provide recommendations to remediate deficiencies. Install, configure, monitor, and maintain McAfee Intrusion Prevention Systems. Install and configure FoundStone scanners remotely. Utilize FoundStone and Nessus to scan systems. Provide customer service to various divisions around the world. * Configured Red Hat Linux to use Active Directory credentials using Winbind and Samba * Vulnerability Scanning using FoundStone and Nessus Government contractor ERC, Inc September 2004 to March 2011 Sr. Data Analyst In support of NASA's John C. Stennis Space Center: Provide the application of IT security principles, methods and security

products to protect and maintain the availability, integrity, confidentiality, and accountability of information systems that include sensitive (ITAR) data. Implements and advises on IT security policies and procedures to ensure protection of information. Harden UNIX (HP-UX) and Linux workstations to exceed Center for Internet Security (CIS) guidelines. Harden Windows workstations based on Federal Desktop Core Configuration (FDCC). Develop System Security Plans for High Pressure Gas, High Pressure Industrial Water, and E-Complex Data Processing at the John C. Stennis Space Center based on NIST 800-53/53a series. * Provided crucial support in the retrieval and analysis for the solution of a reoccurring sensor problem on the space shuttle that had the potential for catastrophic failure (Loss of Life or Vehicle). * Systems Administration (HP-UX, Linux, Windows) * Produced IT Security briefs for company in support of the service contract. * Scanning, vulnerability assessment, and remediation for NASA workstations. * Held Secret Clearance Previous Successes: Lockheed Martin / John C - Stennis Space Center, MS September 1994 to August 2004 Sverdrup Technology / John C - Stennis Space Center, MS September 1987 to August 1994 Computer Science Corp / John C - Stennis Space Center, MS August 1982 to August 1987 Education Bachelor of Science in Mathematics in Mathematics University of Southern Mississippi - Hattiesburg, MS Skills FIREWALL, INTRUSION, SYSTEM ADMINISTRATION, GIAC, INTRUSION DETECTION Links http://www.linkedin.com/in/fkabell Additional Information Critical Skills: * 5 SANS/GIAC Certifications * Risk Assessment & Contingency Planning * Vulnerability Scanning * System Administration * Web Application Firewall * Communication Skills * Intrusion Detection * User Training and Support

Name: Ricky Rojas

Email: tiffanycline@example.net

Phone: 426.822.4292