IT IRM: Security Analyst/ Security Incident Investigator / Soc Analyst IT IRM: Security Analyst/ Security Incident Investigator / Soc Analyst Senior IT Security Analyst Atlanta, GA Dear Hiring Manager, I feel that my skills and experience are a great fit for this position. Please feel free to contact me to arrange an interview. I look forward to learning more about this opportunity.As a certified Network Security Engineer I would bring a comprehensive understanding of the latest networking platforms and the perspective of a computer hardware expert to your organization. In my current position I am required to log all security incidents and then resolve each one as quickly and completely as possible. My eye for detail and my dedication to finding the right solution to a given problem have given me a reputation for success in my field. I am also known for working long hours and completely analyzing a problem to prevent a recurrence.Your company has seen rapid expansion over the past 12 months and you require a Information Security Analyst with my credentials to keep your network secure. I spent more than a year developing the manual for IT Security at my current company and that manual is used to train new technicians at company locations around the world. I would bring that level of experience and expertise to your organization.

My innovative and effective approach to being a IT Security Analyst is what makes me the best candidate for your organization. I await contact from you to discuss my credentials and arrange a meeting at your earliest convenience. thanks & regards, Srujan kumar munangi. Authorized to work in the US for any employer Work Experience IT IRM: Security Analyst/ Security Incident Investigator / Soc Analyst coca-cola - Atlanta, GA May 2017 to Present Monitor network traffic to detect and mitigate any potential threats. Analyze alerts triggered via the SIEM Tools. Investigate and analyze malicious traffic reported by local Host Intrusion Detection System. Investigate and Hunt down compromised accounts and Conduct proactive monitoring, investigation, and mitigation of security incidents. Analyze security event data from the network (IDS, SIEM). Perform static malware analysis on isolated virtual servers. Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Processed Data Loss Prevention (DLP) events in Exchange Rules to identify any violation of the Security Policy , Search firewall, email, web or DNS logs to

identify and mitigate intrusion attempts. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Proposed and tuned out use-cases for better monitoring. Assist in managing hosts through Microsoft Tools. Leadership Achievements: Used and maintained various security tools Trained Tier 1 on how to analyze security threats and understand security concepts Created a PowerShell script that deletes the mass phishes based on any given string. Developed multiple knowledge base documents that resulted in a faster resolution for users Analyzed security threats for managed services customer networks Monitored SIEM tools for threats and vulnerabilities. Review All Incidents and alerts created Solved various security threats for customers. Automated use cases to create alerts and reports, Worked to Automate use cases, created Dashboards, alerts and reports through Splunk. Worked on Web Application Assessment and assisted Application Security Assessment team to provide remediation Based on OWASP and SANS top Vulnerabilities Conducted Pentest on web applications using Burp Suite and Automated test using App-Scan IT Security Consultant HCL Technologies April 2013 to November 2014 Continuously involved with mitigating malware on user machines. Reviewed security and event management logs within the enterprise and investigate suspicious activity through various data visualizer on Qradar Monitored antivirus/Antimalware server consoles such as Malwarebytes for malware remediation and network sensors for lateral movement within the enterprise. Education Masters in Info, Network & Comp Security NYIT - USA, NY January 2015 to December 2016 Skills MySQL (2 years), Splunk (2 years), Exchange Operations (2 years), Symantec (2 years), Fire-Eye analyst (2 years), Network Security (2 years), Powershell (Less than 1 year), defender ATP (Less than 1 year), Source fire Analyst (Less than 1 year), Service Now Incident Management (2 years), Information Security, It Security, Cyber Security, SOC, Incident responder (2 years), pentest (Less than 1 year), burp suite (Less than 1 year), app scan (Less than 1 year) Certifications/Licenses CEH Additional Information Hands-on experience with SIEM Tools like-Splunk, Symantec, Windows Defender ATP, exchange ATP, Advanced Threat analytics, Fire-EYE, Service Now, Symantec ATP, Exchange Admin tools, Sourcefire, Netwitness Programming skills in Java, Python, and SQL

Name: Jay Butler

Email: nstokes@example.com

Phone: 866-483-5849x89379