Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Wipro Frisco, TX Security Analyst with over 2 years of experience and expertise in IT and over 1 year experience in monitoring network infrastructure using QRadar and Azure Security Center. Proven record of evaluating system vulnerability, compiling actionable analysis, reporting threats and escalating it to tier 2 engineers Authorized to work in the US for any employer Work Experience Cyber Security Analyst Wipro - Plano, TX February 2017 to Present Performed real-time monitoring, security incident handling, investigation, analysis, reporting and escalations of security events from multiple log sources using SIEM tool called QRadar. ? Provided information regarding intrusion events, security incidents, and other threat indicators and warning information in a ticket using Service Now ticketing tool. ? Documented all activities during an incident and provide support with status updates of incident. ? Implemented, as directed, appropriate response measures to security threats. ? Analyzed a variety of network and host-based security appliance logs (Firewalls, Work Stations, AD) to determine the correct remediation actions and escalation paths for each incident. ? Categorized support problems and responded with the appropriate level of urgency. ? Defined and update security standards and checklists. ? Worked with various departments to improve detection of security threats and breaches. IT support / Asset management Raytheon / CSC - Dallas, TX 2016 to 2017 Provided troubleshooting assistance and ticket resolution for personal computer users. ? Supported computer users with installation of basic hardware and software. ? Diagnosed and troubleshoot problems with individual or multiple computer systems in order to maintain proper functioning. ? Assisted with computer studies, projects, and implementation of policies throughout area of assignment. Education Bachelor of Science in Information Technology and security Northeastern Illinois University - Chicago, IL 2012 to 2016 Skills integration. (Less than 1 year), INTEGRATOR (Less than 1 year), operations (Less than 1 year), Security (1 year), SIEM (1 year) Additional Information Skills ? Experience in SOC environment ? Knowledge of SIEM tools such as Qradar and Splunk. ? Understanding of TCP/IP, ports and protocols. ? Log source integration. ? Ability to excel in a face paced, challenging, operations environment with 24/7 shifts ? Ability to administer the operations of a security infrastructure ? Multi tenant environment and

shared service model exposure. ? Work per Cyber Kill Chain model.

Name: Matthew Garza

Email: twhitehead@example.org

Phone: 001-757-932-6764