Cyber Security/ IT Analyst Cyber Security/IT Analyst Cyber Security/ IT Analyst - The Nigbel Group Houston, TX A technologically-savvy individual with deep interest in cybersecurity, information technology, process improvement and change management. Proven and demonstrated ability to effectively act as a first-level incident response handler in an organizational setting. A well-educated and exposed individual with high aptitude who demonstrates attention to detail and competency in mastering new systems and technologies. Highly adaptable and proficient in a wide array of security monitoring tools. Authorized to work for any employer in the US. Willing to relocate anywhere within the US. Alerts and reviews Log monitoring Intrusion detection Report rendition Scheduling Analysis and correlation Malware Analysis and Classification Penetration tests Intrusion prevention Process Improvement Work Experience Cyber Security/ IT Analyst The Nigbel Group - Houston, TX April 2016 to Present SIEM Monitoring and SOC Operations -analyzes security event data from SIEM tool, IDS, IPS, firewalls and router (e.g. Arcsight, SolarWinds) to get the right balance between caution, false positives and incidents, while providing effective security monitoring and incident response through triage, investigation, communication, reporting and escalation Analyze and respond to/escalate cyber security incidents and analyze full PCAPs from security logs Initiate incident notification, case tracking/management, recovery actions and escalations where applicable within SLAs using ServiceNow Performs initial incident investigation to be used by Tier 2 Security Analyst for event investigation Initiate incident notification, case tracking/management and recovery actions Hands-on experience managing IP networks, intrusion detection sensors (host and network), intrusion prevention systems and firewalls Perform trouble shooting using TCP/IP knowledge to diagnose and isolate common network issues Document actions in tickets to effectively communicate and track information with team members and internal customers Document, follow and improve policies, procedures and best security practices Work with supervisor to resolve issues and follow documented escalation procedures Review internal logs and alerts to determine and detect potential cybersecurity events. Triage cases based on output from automated alerts, and determine when to escalate to tier 2/3 resources Alongside supervisor, interface with customers to consult with them on best security practices and help them

mature their security posture Risk Management Framework (RMF) Assessments: Perform risk analysis around risk management framework (RMF) NIST 800-37 and support applicable laws and authorization to operate process in accordance with industry accepted regulations and standards relating to security Controls and Assessments: Performs and validates Security Controls in accordance with industry standards Education Postgraduate Diploma in Global Human Resource Management University of Liverpool 2014 BSc in Microbiology University of Benin 2007 Skills customer service (5 years), Dns (3 years), Excellent written (Less than 1 year), Http (3 years), Ids (3 years), incident response (3 years), intrusion (3 years), intrusion detection (3 years), Ips (3 years), metrics (4 years), Networking (3 years), Nist (3 years), organizational skills (5 years), Security (3 years), Siem (3 years), Solarwinds (3 years), Tcp (3 years), Tcp/ip (3 years), Microsoft Office (10+ years), training (5 years), HTML, Active Directory (3 years), Cisco, CompTIA Security+ SYO-501 Certifications/Licenses CompTIA Security+ SYO-501 July 2019 to July 2022 CompTIA Security+ is a global certification that validates baseline skills you need to perform core security functions and pursue an IT security career. https://certification.comptia.org/certifications/ security

Name: William Wilson

Email: shafferalexis@example.net

Phone: 5073334386