Security Analyst Security Analyst Security Analyst - Whois, Shodan, DNS Oklahoma City, OK Authorized to work in the US for any employer Work Experience Security Analyst Whois, Shodan, DNS 2012 to Present with Nmap, Kali Linux, Nessus** Monitoring Completed systems configuration for Windows and Linux operating systems and evidence Performed security base lining for compliance with company policy and standard collection: Wireshark, security practice using tools like MBSA NetworkMiner** SIEM Create schedule for HIPAA, PCI audits for PII data controls and related regulations Tools like Alien Vault Configure log centralization into SIEM tools such as Splunk and Alien Vault OSSIM, Splunk** Intrusion detection Assisted with Disaster Recovery plan review, Business continuity plan testing systems(IDS and NIDS) Monitored incident/event management systems and initiated, resolved and escalated systems: Snort and security incidents per established process Security Onion** DLP Performed packet capture using command line options and GUI tools like Wireshark implementation, and tcpdump. Analyzed captured traffic in relation to source and destination IP, Ports monitoring CuSpider for reported security events/incidents and myDLP to protect Perform system analysis for reported security incidents like DOS, Brute Force attack sensitive data** and social engineering events Networking: DNS, Complete email review for suspected phishing and social engineering attacks with TCP/IP, DHCP, Netstat, approved tools/applications Tcpdump, Windump, NetBIOS ** Encryption Designed proactive scanning for systems analysis based on known trends and and hashing techniques suspected malicious traffic. Deployed NIDS sensors based on location of critical SHA and MD5 network systems and identified emerging trends methods** Windows and Unix operating IT Security Analyst IT Security Professional at Page Technologies 2010 to 2012 Configuration** Policy Management policy Configured HIDS for mission critical network systems and applications with sensitive design and and proprietary data implementation** Configured centralized intrusion prevention systems management based on defined Network intrusion hosts IP, protocols and networks with pfSense prevention firewall Design vulnerability assessment and scheduling for applications and operating systems (IPS and NIPS) systems with Nessus and OpenVAS. Review vulnerability assessment reports - pfSense** Microsoft Office suite(Word, Installed, configured

and maintained of scanning applications Excel, PowerPoint)** Monitored security patch levels of the servers, workstations, and network Programming with R environments and anti-virus systems language** Engineering Developed coordinated, implemented and maintained standards and procedures to design and analysis protect the security and integrity of information systems and data (Corel, WaterCAD, Provided detailed status updates on exiting cyber security incidents to include AutoCAD, MINEQL + ** follow up with clients Reviewed websites for firewalls to determine their proficiency in cyber crime Scheduled and tracked all external audits and assessments process Spearheaded creation of four new information- security departments; Risk Assessment, Penetration Testing, Vulnerability and Security Engineering services Education Bachelor of Engineering in Engineering University of Oklahoma - Norman, OK May 2013 to December 2017 Bachelor of Science in Geology in Geology University of Calabar December 2001 to May 2005 Skills printing (Less than 1 year), Security (8 years) Additional Information Skills Experienced professional with knowledge in engineering systems and information Foot printing, technology security management enumeration and reconnaissance -

Name: Jessica Austin

Email: xmerritt@example.net

Phone: +1-564-968-7014x390