IT Security Analyst IT Security Analyst Wheaton, MD I am goal and detail-oriented professional and expert in cyber security related activities (detect, analyze, respond, recover). My exposure to different training and environment shaped my knowledge when it comes to the use of cyber security frameworks such as NIST SP 800-37, NIST SP 800-39, NIST SP 800-53, and other applicable guidance. Work Experience IT Security Analyst Amtrak - Washington, DC August 2018 to Present Cyber Security Operator deployed to critical incidents and response. Investigates, researches, reports, and analyzes cyber threats, attacks, and events. Mitigates operational threats and provides follow-up incident and technical reporting. Presents briefings to senior leadership and summary reports on the cyber security operation activities. Coordinates and prepares courses of action (COAs) for containment, isolation, and recovery, analyzes and preserves data for required follow-up and analysis. Full and expert knowledge of cyber incident and response/reporting lifecycle. Minimizes any damage or impact to information networks, systems, data, and services. Coordinates and communicates cyber incident information through appropriate channels and with appropriate stakeholders and organizations. Recovers affected systems and assists in the return to a fully functioning, secure, operational state for all services and systems. Understand patterns of activity, best practices, and trends to characterize the threat and direct protective and defensive strategies and prevent a reoccurrence of the cyber event/incident. Complies with preliminary response actions, first responder actions, to preserve and protect incident artifacts and evidence/chain of custody. Conducting monthly AD report to uncover unauthorized accounts and discrepancies. Creating and updating incidents, service requests, and change request tickets using a centralized tool. Creating, developing, updating SOPs for accuracy and correctness. Contributing to developing, updating, and overseeing user's awareness training program. Working closely with the SIEM administrator to fine tuning rules in order to reduce false positive and increase overall performance. Conducting investigation on malicious emails and responding according to the SOP in place. IT Security Analyst Marriott International April 2016 to July 2018 Provided detection and troubleshooting support for security events/incidents. Used Splunk to monitor, analyze and provide reporting through various data sources such as network logs, Syslog, firewall

logs, IDS/IPS logs and NetFlow data. Performed in-depth analysis, response and remediation on cyber incidents and events in the day-to-day monitoring of the company global technology environment; determined course of action in compliance with the appropriate operational level agreements. Provided independent thinking and real-time decision making to diagnose and analyze incidents ensuring critical response and remediation. Performed in-depth analysis, monitoring, research, assessment and recommendations on intrusion detection and prevention tools, anomaly detection systems, firewalls, antivirus systems and proxy devices. Provided log/network/malware/device analysis and made recommendations for remediation of security vulnerability identified. Leveraged commercial and open source tools to quickly analyze, detect, and respond to cyber security incidents. Developed and maintained documentation as a result of complex threats and incidents to enhance event monitoring and incident response functions and cyber tools, including standard operating procedures (SOPs), playbooks, and operational metric reports. Education Master of Science in Information Systems in Network Security Bowie State University December 2017 Bachelor of Science in Finance and Auditing in Finance and Auditing University of Ouagadougou October 2012 Skills detail-oriented (Less than 1 year), organizational skills (3 years), problem solving (3 years), scripting (3 years), team player. (3 years), time management (3 years) Certifications/Licenses CompTIA Security+ February 2018 to February 2021 Additional Information ? Experienced in the development of System Security Plans (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, and Configuration Management. ? Experience within the SOC environment ? Plans, System Security Checklists, Privacy Impact Assessments, POA&M ? Familiar with VMware and other Virtual Machine Applications ? Good communication and writing skills ? Experienced working with NIST SP 800-37, NIST SP 800-53, NIST SP 800-39, FIPS 199, ? Familiar with the following technology: CISCO ASA Firewall, SolarWinds, LogRhythm, Splunk, Microsoft Office 365, CrowdStike, AlertLogic, Akamai Web Application Firewall, Palo Alto wildfire, AppDynamics, Business Direct IDS, Netskope. ? Familiar the following Operating System: Windows 7, Window 8, Windows 10, Linux, MAC OS Additional Skills: Highly-detail-oriented individual with ability to work independently or as part of

multiple teams. Strong organizational skills and ability to stay focused while managing multiple tasks concurrently. Self-motivated and able to demonstrate excellent time management and organizational skills. Strong critical thinking/Analytical skills, creativity, and a proven drive for quality Quick learner. Strong problem solving and analytical skills Great team player. Good knowledge of python scripting language

Name: Angela Cherry

Email: torresjennifer@example.org

Phone: +1-846-462-6444x2433