IT Help Desk IT Help Desk Newark, NJ An experienced Cyber Security Professional with over 3 years of experience in Security Operations processes, incident/event management and threat analysis. Possess working knowledge of vulnerability management and patch implementation. Has experience with console monitoring and detection tool for incident management and response using Intrusion Detection (IDS) as wells as Intrusion Prevention (IPS) systems. Work Experience IT Help Desk Livingston, NJ 2017 to Present Assisted end users with Archer usage issues, and completing break-fix requests using ITSM tools Completed systems configuration for Windows and Linux operating systems Performed access control review and management for multi-factor authentication Knowledge of user profile management in Active Directory and GPO settings review Recommended changes to strengthen information technology, internal controls/business process controls and operating effectiveness. Network resource management including printer and device configuration Incident Management including triage, assessment and escalation based on criticality Utilized strong communication skills (verbal and written) to communicate complex issues to technical and non-technical audiences Assisted with process documentation of critical operations for rapid problem resolution Help transfer in-coming calls to designated places, including patience rooms Add and remove patient from the system (hospital census) as instructed by the Administrators Security Operations Analyst Luisa Home Health Care and Nursing Services - Atlanta, GA February 2015 to June 2019 Performed security base lining for compliance with company policy and standard security practice using tools like MBSA Create schedule for HIPAA, PCI audits for PII data controls and related regulations Configure log centralization into SIEM tools such as Splunk and Alien Vault Assisted with Disaster Recovery plan review, Business continuity plan testing Monitored incident/event management systems and initiated, resolved and escalated security incidents per established process Performed packet capture using command line options and GUI tools like Wireshark and tcpdump. Analyzed captured traffic in relation to source and destination IP, Ports for reported security events/incidents Perform system analysis for reported security incidents like DOS, Brute Force attack and social engineering events Complete email review for suspected phishing and social engineering attacks with approved tools/applications

Designed proactive scanning for systems analysis based on known trends and suspected malicious traffic. Deployed NIDS sensors based on location of critical network systems and identified emerging trends Configured HIDS for mission critical network systems and applications with sensitive and proprietary data Configured centralized intrusion prevention systems management based on defined hosts IP, protocols and networks with pfSense Design vulnerability assessment and scheduling for applications and operating systems with Nessus and OpenVAS. Review vulnerability assessment reports Sample artefacts created include: Project Requirement Document (PRD), Current and Future State Business Process Flows, Business Scenario Analysis Documents, and Business Use Cases. Used Scrum to formalize software development projects that was able to work for any complex, innovative scope of work. Prepare guidance policies and procedures for business units as needed to ensure business units are in compliance with federal, state and local regulatory requirements Skills Business continuity, Disaster recovery, Dlp, Ids, Ips, Iso, Nessus, Nexpose, Nist, Nmap, Pci, Sox, Siem, Snort, Splunk, Tcpdump, Wireshark, Business continuity planning, Firewalls, Security Additional Information Technical Skills: Network Monitoring and Scanning Knowledge of IT Infrastructure MS Office Suite Foot Printing and Enumeration SDLC (Agile Scrum methodology) Vulnerability Management Regulations (SOX, PCI, GDPR, GBLA) Disaster Recovery Planning Business Continuity Planning Standards (ISO, NIST-800) SIEM Monitoring Traffic Analysis Incident/Event Management Knowledge of IT Protocols IDS (HIDS, NIDS) IPS (HIPS, NIPS) TOOLS: Scanning (Nmap, Currports, Core Impact) SIEM (AlienVault, Splunk) Traffic Analysis (Tcpdump, Wireshark) Vulnerability (Nessus, Openvas, Nexpose) Email Protection (Promox) DLP (Comodo DLP, CuSpider) IDS (Snort, Host Based IDS) IPS (PfSense, Windows/Unix Firewalls) Monitoring (Logrhythm, Sguil, Squert) Security Onion and Kibana Web Application (OWASP, Acunetix) Fireeye (Endpoint Security Tool)

Name: Jacqueline Gonzalez

Email: hernandezeric@example.org

Phone: +1-635-571-2963x0906