Senior Analyst, IT Security Senior Analyst, IT Security Senior Analyst, IT Security - SOC Buford, GA Work Experience Senior Analyst, IT Security SOC - Atlanta, GA January 2017 to Present SecureWorks ? Analyze alerts/logs from multiple device types and vendors. Identify, under strict time-constraints, the salient points of these alerts in order to make a determination as to the threat level and client impact of the alerted activity ? Research vulnerabilities and work with clients to understand the nature, potential impact, and next steps to respond to security incidents ? Perform manual correlation of device logs for greater context into the activity that surrounds a given security event ? Compare IDS signatures with raw PCAPs to determine if an event is a match for both the content and the intention of the signature. ? Join regularly scheduled tuning calls with enterprise level clients. These calls allow us to build a relationship directly with client and discuss their perspective on the services SecureWorks provides. Primary goals included performing proactive analysis to determine what events are truly impactful/actionable, tune out the events that are not, and customize event handling and escalation paths for high priority incidents. ? Perform trend analysis across all client activity (More than 110 billion new events per day) to make determinations regarding all client's handling policies based on fidelity, impact, and actionability ? Work directly with developers to identify potential improvements in proprietary tools/platforms Health Infrastructure Monitoring Team Lead ? Interpret and implement customer change requests on managed security device platforms ? Assigned daily shift responsibilities to my fellow team members by prioritizing tickets to meet the team objectives ? Made sure service level agreements related to device change implementation are met ? Remotely access and manage devices at various global customer locations from a security operations center ? Acted as point of escalation to our clients whenever there was service delivery satisfaction issue ? Opened an incident response ticket for all incidents and open a service ticket for all service requests. Monitor all tickets from creation to resolution to closure ? Support activating new client accounts through the provisioning/installation of firewalls or IDS/IDP ? Services monitored included, but are not limited to SIEM, IDS/IPS, Firewalls, Web Application Firewalls, Windows Servers, Cisco ASA Firepower, Sourcefire, Lastline, Carbon Black server. ? Investigated and troubleshoot devices that stopped

logging ? Managed or directly worked on projects, assignments, or initiatives assigned by management ? Conducted in-house training/ride-alongs to groups from outside the SOC to foster an understanding of the Infrastructure Health Monitoring role within SecureWorks IT Technician CenRAS - Providence, RI January 2014 to January 2016 Center for refugee advocacy ? Installed and maintained computer operating systems hardware and software packages ? Created user accounts, and security groups, assigned permissions, deployed client workstations to network ? Ensured security of the system, allowing user zero clients onto system through port security ? Utilized Active Directory to develop and modify user account profiles ? Verified fresh hardware and software for compatibility with organization systems ? Responded to and resolved computer system problems as required Staff Accountant Randstad - Providence, RI 2013 to 2014 Fellowship Health Resource, Lincoln, RI ? Prepared, audited, and analyzed accounting records, financial statements and other reports ? Strictly adhered to stringent accounting regulations and procedural standards ? Operated and managed computers with accounting software to record, store, and analyze information ? Verified figures, postings, and documents for correct entry, mathematical accuracy and proper codes ? Classified, recorded, and summarized numerical and financial data to compile and keep records, using journals and ledgers and computers ? Completed all paperwork, documentation and records with careful attention to confidentiality, met deadlines Family Grocery Shop Retail Owner Lusaka, ZM 2002 to 2006 Education Bachelor of Science in Computer Information Systems/Accounting Rhode Island College - Providence, RI 2013 Skills security Additional Information * Multilingual - Fluent in English, Kinyarwanda (Native), Swahili, Kirundi, Nyanja

Name: Melanie Watson MD

Email: andrewmurphy@example.org

Phone: 3154563769