IT Security Analyst IT Security Analyst IT Security Analyst - Southern Company Suwanee, GA Work Experience IT Security Analyst Southern Company - Atlanta, GA March 2014 to Present Worked all roles within the SOC; Threat Analysis, Incident Response, and Insider Threat. Currently working primarily as a Threat Analyst my function is to find network anomalies, investigate events, and create/escalate/finalize these cases while interfacing with the other roles and business units. Objective is to be proactive in the protection of our high value targets which include proprietary data and critical infrastructure. Work in depth with multiple security technologies including Arksight, Splunk, Palo Alto, Bluecoat Solera, Sourcefire, Tanium, ProofPoint, Exabeam UBA, and other cybersecurity tools. Create cases with Remedy to manage and remediate an array of security events within specified SLE's to protect the Southern network environment. Create/Update Incident Response Plan documentation; Work in depth on the incident response team to identify and remediate threats to the Southern Company environment. Process intelligence from multiple vendors to provide Situational Reports on our security posture for upper management. Work with compliance and corporate security teams on investigations that include data exfiltration, inappropriate behavior, and various other illegal activities. Work closely with our content team to assist in tuning rules by defining network zones/resources and creating a baseline of network traffic.

Train new employees on security techniques, policies, and procedures. Global Operations Manager IBM - Atlanta, GA April 2012 to March 2014 Managing the daily operations of the Security Operations Center with a team of 32 firewall engineers and security analysts in 5 global geographical locations to provide security services to our customer base and the management of over 4,000 security appliances and firewalls. Management of exempt and non-exempt personnel, recruitment and hiring of new personnel to ensure proper staffing levels, developing training plans, providing performance reviews, real-time feedback, and assisting in career planning and promotion opportunities for team members. Maintaining the quality of all customer communications, handling customer escalations, maintaining productivity standards, scheduling appropriate resources, and managing special assigned projects. Identifies needs, develops, and creates procedures to improve policies, workflows, and systems required for the Security Operations Center's efficient and

professional operation. Collaborate and engage in communication with upper management and personnel from other MSS groups (Deployment, Customer Advocacy, and Engineering) to ensure that customer concerns/expectations are met. Work with the customer to understand issues, requirements and responds to requests for new services (Request for Service-RFS's) to help grow the business. Establish and maintain metrics that help provide assistance with managing at a high level of productivity, supportability, and operational readiness. Escalation Engineer IBM - Atlanta, GA February 2011 to April 2012 Troubleshoot device outages, network connectivity issues, policy and VPN related problems. Tuning and maintenance for managed devices: Cisco Pix/ASA/FWSM, Check Point NGX/UTM, ISS Proventia A/G/M appliances, Juniper NetScreen/IDP/ISG/SRX, and BlueCoat web proxies Perform system upgrades for multiple platforms: Proventia, Cisco, and Check Point appliances Perform firewall policy change requests for multiple platforms: Proventia, Check Point, Cisco, Juniper, and BlueCoat appliances Perform Quality Assurance checks for newly deployed customer devices Perform verification of policy change requests Comprehensive network monitoring with Nagios Security Analyst Secureworks - Atlanta, GA September 2010 to February 2011 Monitor Intrusion Detection System (IDS) data and firewall security alert data logs and identify security incidents Notify customer of security incidents within SLA and discuss corrective actions to be taken. Troubleshoot device logging issues and correct problems to ensure that devices are logging properly into SOC environment. Identify false positives in log data and create filters for managed devices Perform system and signature updates for iSensor IPS appliances Team Lead - Device Management Group IBM May 2008 to September 2010 Managing the nightly floor operation of a 10 analyst/ escalation engineer staff to provide IT security and device management services to clients for the IBM Managed Security Services organization Ensure that all nightly scheduled DMG maintenance events are staffed properly with appropriate skilled personnel and the maintenance is performed correctly. monitoring all device management ticket queues to ensure that sure nightly service level agreements are met Monitor the MSS-SOC-Escalations distribution list for DMG related customer escalations and ensure that concerns are addressed within the internal MSS SLO requirements. Ensure that all inbound DMG

queues are staffed adequately with resources and that phone/chat queues have proper resources available. Ensure that nightly staffing levels are properly maintained. In charge of approvals for staff vacation requests Training of new personnel and interviewing prospects for new position within the MSS organization In charge of upgrade project for the Cisco ASA/PIX appliance platforms Perform Policy Change Requests and assist in Policy Change Verifications on multiple platforms including Cisco, Juniper, Checkpoint, and Proventia devices Escalation engineer IBM - Atlanta, GA October 2004 to September 2010 Security Services Analyst IBM October 2004 to May 2008 Monitor of Intrusion Detection System (IDS) data utilizing Site Protector. Perform monitoring of firewall security alert data logs and process policy change requests for multiple firewall platforms as requested. Identify security incidents, notify customer and discuss actions to be taken. Responsible for QA, tuning, troubleshooting, and maintenance of security devices and management of security policies Troubleshooting device outages, connectivity issues, and security policy related issues. Research and assess new threats and security alerts and recommends remedial action Perform policy tuning on security device policies Process Policy Change Requests on multiple platforms, including Checkpoint, Juniper, and Cisco appliances. Senior Computer Operator Infinity Property & Casualty Company - Atlanta, GA September 1997 to July 2004 Responsible for monitoring and balancing nightly policy management system and financial batch cycles. Perform weekly system backup and restore. Monitor Unix ITO and Omniback processes. Conduct mainframe to PC file transfers, NT/Arcserve backups, SQL downloads, tape management and system IPLs. Train new employees within the Data Operations department on systems, office procedures and protocol. Computer Operator Mobile, AL August 1989 to August 1997 Responsible for batch processing of financial, payroll, overhead and warehouse information. IBM mainframe environment with VM, VSE/ESA, VTAM, CICS and Xerox/IBM peripherals. Provide technical support for software/hardware problems occurring at the store level chain wide. Involved in training new employees hired in the MIS department Education B.A. in Criminal Justice University of South Alabama - Mobile, AL Certified Support Professional Kennesaw State University Skills Security, access

Name: Dr. Annette Goodman

Email: hendersonjose@example.net

Phone: 001-737-249-7721x92095