Tier 1 Security Analyst, Security Operations Center (SOC) Tier 1 Security Analyst, Security Operations Center (SOC) Tier 1 Security Analyst, Security Operations Center (SOC) Morrisville, NC Work Experience Tier 1 Security Analyst, Security Operations Center (SOC) Cisco - Morrisville, NC June 2018 to August 2018 * Continuously monitored the alert queue for multiple-sized clients, from small companies to large universities using multiple tools, such as IDS/IPS, Packet Capture (PCAP), SIEM, and custom-built network monitoring tools * Analyzed raw data for potentially malicious behavior by inspecting logs from IDS/IPS, firewall, ESA & Cisco ASA logs, etc. * Examined Encrypted Traffic Analytics (ETA) using Stealthwatch integration with Cisco Identity Services Engine (ISE) * Utilized ICS Ranger with Claroty platform integration to protect industrial control systems (ICS/SCADA) SecOps by maintaining uptime and documenting captured logs for further investigation * Performed initial triage of alerts to identify potential, false positives, policy violations, intrusion attempts and compromises * Utilized regular expressions for Splunk to analyze machine-generated big data * Researched the latest technologies for intelligence, including hackers' methodologies, to anticipate security breaches * Consolidated data and escalated issues from alert triage in ServiceNow ticketing system to provide context necessary for Tier II & Tier III Analysts to examine and review incidents on a deeper level Information Security Analyst, Security Operations Center (SOC) Hanesbrands Inc - Winston-Salem, NC June 2017 to June 2018 * Providing risk management globally for over 14,000 workstations, servers, and POS devices and benchmarking cybersecurity performance with security rating tools * Adding and configuring log sources from collectors with custom rules and responses with SIEM * Reduced potentially malicious cyber threat alerts with incident mitigation by 90% using deep/dark web monitoring tool * Managing vulnerabilities, incident response, and threat hunting by utilizing SCCM * Preventing advanced threats and data breaches by exploring metadata forensics and analytics using deep packet inspection tools and IDS/IPS * Spearheaded the development of policy creation and modification on security standards to meet government regulations to pass Sarbanes-Oxley (SOX) compliance audits * Generating security reports/metrics based on created vulnerability management and compliance scans using Qualys * Maintain SharePoint internal site and database with current

detailed information regarding IP addresses, locations, contacts, & documentation * Collaborated with vendors to identify and execute security architecture enhancements IT Support, Network Operations Center (NOC) ECPI University - Greensboro, NC January 2016 to June 2017 * Maintained network uptime and availability for over 400 computers on campus * Handled IT services help desk request e-mails and calls in timely manner * Resolved hardware/software issues, network and application issues for end-users * Deployed applications and software upgrades from Windows Server remotely using PDQ Deploy * Re-imaged machines requiring repairs to the operating system * Determined problems with LAN, WAN, or domain connections and implemented resolutions * Managed print quotas and balances for network users through Print Manager Plus Internship, IT Support Technician ECPI University - Greensboro, NC July 2016 to September 2016 * Created ISO images with Sysprep, deployed with appropriate software needed for 10 different locations using Symantec GhostCast Server and PDQ Deploy * Re-organized forest tree in Active Directory by relocating instructors to their new sites * Worked within registry editor and local group policy to allow/deny specific privileges for directors and instructors * Assisted in set-up and configuration of hardware for new PC's and network printer installations at new sites, and connected them to the domain * Handled various hardware/software troubleshooting needs BEGAN CAREER CHANGE BY ATTENDING ECPI UNIVERSITY FOR NETWORK & CYBER SECURITY Customer Care Support/Logistics Coordinator i-Automation - High Point, NC August 2013 to May 2015 * Served as liaison between vendors and purchasing department by verifying part numbers, quantities, and pricing, which led to an annual 15% decrease in shipment errors * Coordinated shipments between vendors and customers * Retrieved and recorded vital logistics related information from purchase and sale order acknowledgements in NetSuite * Created daily missing/late orders Excel reports and maintained goal of less than 100 daily late orders * Assisted purchasing team leader with NetSuite and PowerPoint projects through a comprehensive work of redesign and process improvement for software upgrade to utilize the database more efficiently Education B.S. in Computer and Information Science ECPI University - Greensboro, NC June 2017 B.S. in Business Administration University of North Carolina at Greensboro - Greensboro, NC

August 2011 Skills Security (2 years), Qualys (1 year), SIEM (3 years), Network Security (3 years), Threat Management (3 years), Incident Management (3 years) Links http://WWW.LINKEDIN.COM/IN/JESSEBASSI Certifications/Licenses CompTIA A+ June 2016 to June 2019 Additional Information SKILL SUMMARY * Efficient with Networking, Security Monitoring, Incidence Response, and Vulnerability/Threat Management * Proficient with virtual environments including VMWare, Virtual Box, Citrix Receiver and XenDesktop * Proven track record of efficiency with multiple cyber security tools and programs: ? IBM QRadar ? Fidelis Cybersecurity Threat Detection ? Carbon Black ? Qualys Security & Compliance ? IntSights Dark Web Monitoring Tool ? SCCM ? PowerShell ? Active Directory ? PuTTy ? Cisco Packet Tracer ? Wireshark ? PDQ Deploy ? Splunk ? ELK Stack (for NetFlow Analytics)

Name: Kurt Murphy

Email: longmeagan@example.net

Phone: 755-308-6588