Information Security Analyst Information Security Analyst Information Security Analyst Scottsdale, AZ I m young, intelligent, and ambitious with a passion for learning. Education is very important to me, and I m striving to make an impact on the world. When I set my mind to something, I am committed to achieving my goal. I m outgoing and friendly and can relate well with other people. As an analyst, my strengths lie in spotting patterns, manipulating data, solving problems, and communicating well with my team. Authorized to work in the US for any employer Work Experience Information Security Analyst Republic Services 2017 to Present ? Analyzing, filtering, and transforming machine-generated data with the intent to make informed security decisions ? Creating watchlists, alerts, and dashboards, and then further investigating their abnormalities to discover root cause ? Threat hunting for malware, phish, IOCs, vulnerabilities, and other security related incidents ? Gathering and ingesting threat intelligence data from multiple sources ? Performing malware analysis using a combination of automated vendor sandboxes, REMnux, and Carbon Black ? Assisting with enterprise-wide security procedures ? Communicating regularly with vendors to maintain tools, test new security products, and strengthen vendor relationships ? Documenting step-by-step procedures and training on them ? Onboarding, training, and supervising new hires and offshore team members ? Leading incident response and taking on escalations at the highest tier Tools/Experience: Carbon Black Response, Splunk Cloud, Splunk Enterprise Security, Phantom, Python, API, Anomali Threatstream, Recorded Future, Cylance, Cisco ThreatGRID, Crowdstrike - Hybrid Analysis, Proofpoint (TAP, TRAP), OpenDNS - Umbrella, Linux - REMnux, ServiceNow, Configuration Management Databases (CMDB), Office 365, Active Directory, ObserveIT, DomainTools, Endpoint Detection and Response, Incident Response, process analysis, data analytics, big data and information management IT Field Engineer Modis/Republic Services 2016 to 2017 ? Supported the executive team and all other corporate employees for a multi-site corporate headquarters ? Collaborated with specialized teams to manage, maintain, and design the IT infrastructure of a large enterprise environment ? Administered a large Cisco VoIP environment ? Created and supervised Cisco WebEx sessions for company-wide video conferences ? Monitored, analyzed, and troubleshot an enterprise IT infrastructure using various enterprise tools ?

Configured Cisco switches that were then sent out to replace damaged switches at field locations ? Managed an extensive database of users and security groups within Active Directory ? Received and resolved ticket escalations in the highest tiered support role ? Developed and implemented standardized processes and procedures through documentation creation ? Assisted the information security team with phishing and basic alerts Tools/Experience: Splunk Cloud, Active Directory, Cisco CallManager, Cisco Unity Connection, Cisco Jabber, SolarWinds Orion, ServiceNow Configuration Management Databases (CMDB), Carbon Black Response, Proofpoint, Cylance, Cisco WebEx, Altiris Symantec Management, Symantec Ghost Field Technician/ Systems Administrator Schooldesk/Easy IT 2015 to 2016 ? Administered 13 total sites servers and networks (schools, businesses, and nonprofits) ? Managed identities and access for users and security groups in Active Directory ? Acted as a liaison for the company and their customers to analyze current business systems and identify customer needs ? Troubleshot customer and company devices remotely and on site ? Cabled new network infrastructures (WAPs, ports, patch panels, switches, etc) ? Conducted WiFi analyses to create heat maps (Ekahau) and to analyze radio interference (Chanalyzer) ? Implemented network monitoring systems using PRTG and UniFi ? Constructed distribution groups, calendars, and email accounts using Microsoft Exchange 2010 ? Managed Cisco VoIP phones using Cisco CallManager ? Installed, repaired, and troubleshot Sharp, HP, Konica, and Brother business printers ? File restores, hardware swaps, server maintenance and migration, tablet/phone/laptop support, application virtualization (remote desktop and app-v), configuring terminal services, categorizing tickets Tools/Experience: Active Directory, Group Policy, Microsoft Exchange, Windows Server, Cisco CallManager, UniFi, Cisco networking, DNS and DHCP, endpoint imaging, virtualization Education BA in Psychology Minor in Philosophy and logic University of Colorado Denver - Denver, CO December 2014 Skills Information Security, Cyber Security, System Administrator, Threat Intelligence, Endpoint Detection and Response, Incident Response Certifications/Licenses Splunk Certified User Present Splunk Certified Power User Present Carbon Black Response - Associate Analyst Present Additional Information Training ? Splunk - Fundamentals 1 & 2 ? Splunk - Advanced Searching and Reporting ? Splunk - Using

Enterprise Security ? Splunk - Enterprise System Administration ? Splunk - Enterprise Data Administration ? Carbon Black Response - Introductory Analyst ? Carbon Black Response - Advanced Analyst ? SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

Name: Susan Moore

Email: paulbrown@example.com

Phone: 8995228921