Security Operations Specialist II Security Operations Specialist II Security Operations Specialist II - Aires While I currently reside in Pittsburgh, PA, I'm attempting to relocate to my hometown in Chester County, PA or a surrounding area in order to live closer to my family. Work Experience Security Operations Specialist II Aires - Robinson, PA September 2017 to Present Performed a security architecture redesign by reviewing past and current security products and replacing them with products that best fit the company needs and budget. Created and developed the vulnerability management system for Aires. Responsibilities include scheduling vulnerability scans, interpreting and testing the results, and inputting the vulnerabilities into the ticketing system. Assists with remediation as necessary. Created and developed a time tracking ticketing system, which lets our team lead review time spent on various projects and reallocate personnel resources accordingly. Creates and manages user phishing campaigns, which tests end user's susceptibility to phishing attacks. This includes creating the email templates, launching the campaigns, user training, and writing an executive summary. Installed, configured, and tuned the SIEM installation. Manges and monitors the SIEM for alarms and any tuning changes that occur. Manages the Intrusion Detection System, which includes tasks such as alert review, rule review, alarm creation, and other related tasks. Manages the anti-virus solution, including scan configuration, policy creation, and alert review. Assisted with creating STIGs for MacOS and RHEL via CIS Benchmark Standards. Assists with audit tasks such as client audits, SOC II Type II, and ISO 27001/2. Incident Response Analyst Westinghouse Electric Company January 2017 to September 2017 Performs detailed analysis of SIEM events. Analysis includes correlation of various security appliances and SIEM log aggregation. Copied forensic images for legal matters, keeping proper chain of custody and documentation. Configured multiple virtual environments for incident response use and testing purposes, such as a Cuckoo Malware Sandbox, CentOS hyper-visor, and AlienVault OSSIM installation. Cyber Security Specialist NTT Security - Pittsburgh, PA January 2016 to December 2016 Performed analysis on red flags triggered by IDS's, firewalls, servers, workstations, and other networked devices. Determined if the red flags are malicious or false positive and created detailed write-ups to send to the clients. 484-319-5697 aisherwood@fastmail.com alifesecured.com

Depending on the red flag, investigation may include malware analysis, malware and reputation analysis of IP addresses, payload analysis, and other such tasks. IT/Database Assistant Energy Management Systems - Exton, PA May 2015 to August 2015 Worked in a database conversion process of porting an old FoxPro database to SQL Server. Wrote SQL queries providing statistics to help ensure data integrity and for troubleshooting assistance. Worked in an exchange server conversion reconfiguring company devices. Took care of various day to day IT tasks such as desktop support, meter readings, and rebuilds. Automated Meter Reading Specialist May 2014 to August 2014 Obtained utility meter readings using various software on several machines through the use of remote software. Responsibilities included getting meter reads by using VPN's to connect to various sites, troubleshooting software and hardware, data entry, and documenting the previously undocumented process in its entirety. Intern Frontline Placement Technologies - Exton, PA June 2012 to August 2012 Performed day to day tasks the network administrator gave to me. Examples include: making and running Ethernet cabling, setting up PC's, and rebuilding PC's. Set up a lab environment that involved connecting several client machines to a switch, connecting the switch to a couple Windows 2008 R2 servers, and configuring the servers to function as the Domain Controller, DNS, and DHCP for the lab network. Education B.S. in Applied Internet Technologies Liberty University - Lynchburg, VA December 2015 Links https://www.linkedin.com/in/anthonyisherwood Certifications/Licenses Security+ CySA+ eJPT Additional Information SKILLS Experienced in planning and implementing network security architecture. Experienced in configuring and managing SIEMs, NIDS, HIDS, firewalls, and other security appliances. Experienced working with: AlienVault, ArcSight, LogRhythm, Palo Alto NGFWs, Extrahop, Darktrace, Suricata, Webroot, McAfee, Redline, and other various security appliances. Working knowledge of various scripting languages such as Bash, PowerShell, Ruby, and Python. Working knowledge of penetration testing. Experienced in creating projects and custom workflows in Jira. 484-319-5697 aisherwood@fastmail.com alifesecured.com Quick minded and eager learner, always willing to learn something new. Consistently noted by supervisors for outstanding job performances, reliability and multi-tasking skills exhibiting efficiency,

accuracy, speed and timely completion of all assignments. 484-319-5697 aisherwood@fastmail.com alifesecured.com

Name: Edward Evans

Email: vargascharles@example.com

Phone: +1-237-808-7670x0071