Security Ops Center IT Security Analyst Security Ops Center IT Security Analyst Security Ops Center IT Security Analyst - Online Business Systems Wylie, TX Authorized to work in the US for any employer Work Experience Security Ops Center IT Security Analyst Online Business Systems - Irving, TX January 2018 to Present Currently employed as a IT Security Analyst. Monitor application alerts, cyber threats, and then identify and communicate course of action for remediation. Using information derived from alerts on the monitoring console as well as other tools. Research threats with potential impact to clients, generate tickets, and if requested by the client to provide assistance to remediate incidents. Track vulnerabilities found in customer environment and assist with identifying and recommending remediation Conduct research on traffic alerts triggered by SIEM appliances, Azure, and endpoint devices. Continuously monitor alerts generated by security information event management (SIEM) systems and tools. Detect, research and respond to security incidents quickly and accurately. Interact professionally with clients acting as an extension of their security team. Develop customized client reports when necessary. Develop documentation for new analysts to follow as part of training Train and mentor up and coming analysts Security Ops Center Network Security Analyst Masergy Communications - Plano, TX April 2016 to January 2018 3rd Shift Lead I was employed as a Network Security Analyst. Monitor for changes in cyber/human activity, security application alerts, vulnerabilities, cyber threats, and then identify and communicate course of action for remediation. Using information derived from alerts on the monitoring console as well as other tools, I research threats with potential impact to clients, generate tickets, and if requested by the client, provide assistance to remediate the issue. Maintain and deliver service according to customer SLAs. Recognize and identify potential threats to the network and systems connected to the network from the Internet and Intranet. Conduct research on IDS alerts/traffic and Vulnerability/Log Monitoring/Vulnerability Scanning. Monitor critical infrastructure across the clients' environments to include firewalls, IDS/IPS devices, virtual networks, vulnerability scanners, VPNs, WANs, disaster recovery sites, etc. Interact professionally with clients acting as an extension of their network security team. Detect, research and respond to security incidents quickly and accurately. Communicate primarily via e-mail but

also provide phone support. Quality of Service / Auditing SOC IT Security Analyst NetBoundary - Dallas, TX August 2015 to March 2016 I worked as an Information Security professional at NetBoundary, an MSSP focused on PCI DSS. I have knowledge using appliances from manufacturers like LogRhythm, McAfee, LogLogic, and Tipping Point. I am interested in security compliance, IDS/IPS, firewalls, SIEM and, network security monitoring. Performs information security analysis work. Work involves monitoring security equipment for internal and client side infrastructure to assist with adherence to industry and regulatory requirements. Works under general supervision, with moderate latitude for the use of initiative and independent judgment. Monitor log appliances for threats and attacks on client's computer networks and transaction systems as well as internal security appliances. Research and respond to security incidents PCI compliance reporting Document security incidents according to defined policies Vulnerability scans using Tripwire IP360 IT Service Desk Analyst Sonic Healthcare USA - Richardson, TX February 2014 to October 2015 Provide first level technical support for Sonic Healthcare employees support laboratory devices/instruments and applications. Support various locations throughout the USA Provided excellent tier 1 support to callers and escalate incidents to the appropriate group when necessary. Diagnose and resolve problems related to: the use of workstation hardware, software applications, peripheral devices, communication packages, host and LAN/WAN connectivity or other problems. Internet browsers, remote access communication packages (e. g. VPN), laboratory information systems applications (Apollo, Antrim) Provide maintenance of users' Active Directory accounts (add, delete, change) following security guidelines. Trained to comply and follow ITIL methodology IT Service Desk Analyst Quest Diagnostics - Addison, TX March 2012 to November 2013 Provided first and second level technical support for employees at Quest Diagnostic. Supported laboratory devices/instruments and applications. Supported an environment of 35000 plus users via telephone, email queue and, self-service tickets. Provided excellent technical support to callers by: Asking initial targeted, broad questions followed by deeper, focused questions. Troubleshooting using all procedures and technology access in place. Use appropriate techniques and tools to log, track, escalate, resolve and then close calls received by the help desk.

Diagnosed and resolved problems related to: the use of workstation hardware, software applications, peripheral devices, communication packages, host and LAN/WAN connectivity or other problems. Internet browsers, remote access communication packages (e. g. VPN). Access Control - Added, deleted, suspended and, unlocked users' Active Directory accounts and mainframe billing applications accounts following security guidelines Comply with ITIL methodology Education Certificate Collin College - Frisco, TX April 2016 AAS in Information System Cybersecurity Collin College - Frisco, TX December 2015 AAS in Computer Business Administration Heald College - Sacramento, CA July 2000 Skills IDS (4 years), SIEM (4 years), TRIPWIRE (Less than 1 year), SECURITY (3 years), ACTIVE DIRECTORY (3 years), Cyber Security, Cissp, It Security, Information Security Links http://www.linkedin.com/in/riveramarco Additional Information Software Applications: HP Service Manager, ServiceNow, Active Directory, Secure Access Manager, Alarm Point, NS Lite, SharePoint, Nagios, Footprints, Tripwire IP360, LogRhythm, Nessus, Carbon Black, CloudPassage Halo, Suricata IDS, Azure (Threat Manager, Cloud Application Security, and Active Directory), Qualys, and Qradar SIEM Operating Systems: Cisco IOS, Windows OS, Entry-level Linux

Name: Jerry Villarreal

Email: zhowell@example.org

Phone: 624-665-3752