Incident Response Specialist Incident Response Specialist Cyber Security Incident Response Specialist Dallas, TX Hobbies include:Information security, information assurance, incident response, ethical hacking; forensics, DFIR Darkweb networks, cryptocurrencies, block chain and ethereum technologies, Decentralized Applications Home Lab setup running Kali Linux, Authorized to work in the US for any employer Work Experience Incident Response Specialist Blue Cross Blue Shield of IL, MT, NM, OK & TX - Richardson, TX January 2019 to Present The development and maintenance of comprehensive incident response plans and processes that minimize the damage resulting from security incidents Creation and delivery of training material to staff and leaders about all facets of the security incident response process Maintenance the incident type and categorization framework Working with teams monitoring and analysis teams to coordinate activities with other stakeholders for containing, eradicating, and recovering from security incidents Develop threat rules and signatures for cyber defense technologies Spearhead the development of innovative approaches to detect, respond to, and eradicate threats; improve the overall ability of the organization to respond to and eliminate threats; and increase effectiveness of analysts Routinely review existing tools for new capabilities or deficiencies and maintain relationships with vendors and formalized partners to understand the latest deployment strategies and trends Identification of security controls or capabilities that will assist in the prevention, discovery, or resolution of future security incidents Set standards for the documentation of activities during an incident, creation of security incident reports, and for conducting post-incident reviews. Create comprehensive security write-ups which describe security issues, analysis outcomes, and remediation techniques to management Facilitate Root Cause Analysis (RCA) analyses between technology and business partners to deliver recommendations which drive continuous improvement of the organization's defensive capabilities. Develop, track, and maintain metrics reporting to enable the organization track security trends and enable leadership. Support response activities associated with a 24/7/365 matrixed team delivering real time security monitoring and response functions Sr. Security Analyst Blue Cross Blue Shield of IL, MT, NM, OK & TX - Dallas-Fort Worth, TX September 2017 to January 2019 Responsible for monitoring multiple feeds in a 24/7

environment to immediately detect, verify, and respond swiftly to cyber threats Working collaboratively with multiple teams and personnel; Being Highest escalation point in the SOC working with other Security Operations Center (SOC) analysts as well as subject matter experts within the larger distributed Cyber defense team including; cyberthreat hunters, threat intelligence analysts and forensic investigators, incident response working with and gaining further insight into a variety of security logs and devices ranging from operating systems to firewalls, network intrusion detection, databases, applications and more gaining more understanding of current real world cyber threats and attack techniques Conduct security investigations into active threats and vulnerabilities of the HCSC environment Produce and implement Monitoring strategies and plans for continuous monitoring utilizing 15-20 security tools. Generate Reports for purpose of Audit, Metrics, tuning, monitoring and for Senior Leadership Tools used include: Interset, ArcSight, Trend Micro Deep Discovery Inspector, Symantec Endpoint Protection, Palo Alto Firewall, Symantec Bluecoat, Service Now, BurpSuite, Wireshark, Cisco Sourcefire, Bricata, ProofPoint, Cisco IronPort, various threat intel platforms/ threat exchanges, BMC ADDM, Firemon,F5 WAF, Network Operations Analyst (NOC) Esurance February 2017 to September 2017 Monitors, responds to, and reports incidents occurring in the company's IT infrastructure. Provides first-line support for a wide variety of systems and processes including Esurance's 24x7 web presence, WAN, and critical servers and services. Use Enterprise tools such as Splunk, App Dynamics, Solarwinds, Microsoft System Center, Symantec Endpoint Protection, Active Directory, SQL Server Management Studio, SharePoint, Automate BPA Server10 Participate in Severity 1 Bridge calls between teams to resolve issues. Also responsible for reporting on issues and performance, performing maintenance, and working closely with the Network Operations Team to improve monitoring, troubleshooting, and response times. Works with Production Support team to run batch jobs and execute PS Tickets. Run queries in SQL and report to team members Documents issues, fixes, and response times.Reports server, network, and systems performance metrics. Works shifts on a rotational basis to staff the NOCC on a 24x7 basis. Works collaboratively and coordinates between technical and non-technical people within and outside of the group. Perform basic

systems testing and operational tasks (installation of patches, network connectivity testing, script execution, etc.) EHR Technical Analyst Addison Health Systems, Inc February 2016 to February 2017 Conducted specialty private practice clinical implementations of WritePad EHR - remote, with follow up schedule. Provided consultation on complete network, server and client workstation setup. ? Resolve Level II and III support tickets including troubleshooting, utilizing database maintenance tools, examining breached environments and infected databases for malicious files and or services, software patching on servers, Analyze environments(client server- peer2peer- RDP- virtual environments) and clinical networks and make administrative level adjustments in said environments for maximum efficiency of WritePad EHR ? Conduct Security Risk analysis of environments where WritePad EHR runs and implement mitigation techniques to prevent breaches of patient data and networks such as minimizing administrative privileges for users, set up a password rotation system for clinics, reviewing audit logs, update Anti Virus definitions, limiting logon attempts from users, confirm that firewalls settings are updated, minimum levels of encryption for PHI sensitive data, Asset Inventory for Servers, workstations, tablets mobile devices, ? Responsible for Implementing disaster recovery plans by introducing daily backup of EHR with both offsite and cloud based backup, Using MosyPro, Carbonite and others, backup Power Supplies for servers, ? Responsible for handling data migration for large clinics and ambulatory surgical centers from old decommissioned servers to new servers and environments ? Setup HIPAA compliant networks with RDP and VPN connections on Windows 2008r2 and 2012 servers, Win 7,8,10 workstations and thin clients in order to provide a HIPAA compliant, safe and reliable environment. ? Microsoft Access based database tasks such as seeking out corrupted tables and erroneous entries ? Some Active Directory roles, users and user groups configuration. ? to scheduling, patient intake, patient examinations, and billing interfaces for providers. Assesment Data Associate Viverae- Vitals March 2015 to March 2016 Manage and work with up to 100 outlook mailboxes at any given time Process documents by reviewing data for deficiencies Manage Sets of Data for around 60 clients in the healthcare field Trained for PHI standards to handle sensitive health info and take safeguards to ensure privacy of customer data. Maintain data entry requirements by following

data program techniques and procedures Accessing and submitting queries through a database via alpha and numeric identifiers Prepare source data for computer entry by compiling and sorting information. Technical Analyst- Dealer Desk Representative Intersection Technologies- F&I Express March 2014 to March 2015 Analyzed support data, XML's, Web Services Logs, user data and provided feedback to Developers, Business Development Teams, Sales and Marketing Teams daily ? Documented Technical problems and managed support desk ticketing system and support data (Zendesk/ Microsoft Excel) ? Responsible for production and install reports outlining overall use of software, common issues and idea for further improvement and workflow. ? Responsible for working with integration partners' development teams to meet client's technical specifications and internal list of standards. ? Successfully Installed, Trained and Supported web based application used at Car Dealerships ? Answered Customer Trouble tickets ? Worked in multiple environments (Test, demo, production,) ? Manage dealership group accounts, individual business accounts and user accounts and user credentials ? Clearly communicated technical solutions in a user-friendly professional manner ? Installed and troubleshot cloud based application (iOS) ? Responsible for demonstrating software to potential new clients. ? Remote Support via Gotomeeting Laptop Repair Tech Level III SMS InfoComm - HP computers subsidiary January 2013 to March 2014 Manually examine and repair computer hardware and peripheral components ? Test functionality and assess problems by operating computer systems or related ? Troubleshoot computer systems problems ? Take apart and re-assemble computer components and parts ? Use small handheld tools such as screwdrivers, voltmeters, etc ? Manually set up computer systems and hardware, and install or re-install software programs and operating systems for computer users ? Managed software bank and images ? Met a quota of diagnosing, repairing, and documenting 8-10 laptops per day with a failure rate of less than 5% ? Troubleshoot laptops for hardware and software issues from customers and clients ? Repaired hardware and dealt with BIOS issues ? Dealt with OS reloading, and imaging software and data migration IT Remote Support, CSR, Repair Technician SMS InfoComm - HP computers subsidiary - Dallas, TX January 2012 to January 2013 Repaired iphones, android phones and dealt with hardware and software issues of iOS and android. ? Other phones/

troubleshooting and maintenance ? Repaired and maintained support for customer laptop and desktops, (windows xp, 7, 8, mac osx,) ? Preformed hardware installation/repair and troubleshooting ? Software installs, Operating system reloads, hard drive imaging and data migration ? Support of repair clients through remote desktop(teamviewer, vnc,) ? Microsoft exchange 2010 activesync setup and user management ? Setting up of customer WAN, LAN, VPN, ? Maintained store's computer upkeep, hardware repair (desktop/laptops). Software maintenance. ? In charge of Online presence upkeep, network setup and support ? Was responsible for scheduling and receiving shipments, making payments to suppliers, and daily closing register tabulations. ? Set up Point Of Sale System with Barcode Scanning technology for inventory ? Responsible for Inventory Management. Education B.S. in CompTIA Security+ University of North Texas - Dallas, TX May 2017 to Present Skills Network Security, Splunk, Linux, Hadoop, Apache Spark, F5 WAF (1 year), Symantec EndPoint Protection Manager (2 years), Bluecoat Web Proxy (2 years), Kibana - elastisearch (2 years), Nist, Information Security, Siem, Cyber Security

Name: Dennis Wilson

Email: susanparker@example.com

Phone: +1-610-579-8824