Security Assessment Support Engineer Security Assessment Support Engineer Security Assessment Support Engineer - L& T Technologies Services \ PepsiCo Plano, TX Work Experience Security Assessment Support Engineer L& T Technologies Services \ PepsiCo - Plano, TX March 2019 to Present Department: Corp Security Risk & Compliance Group Member: MGF/OT- Cyber Security Program Committee: Cybersecurity Solutions Committee Attending weekly internal L&T meeting Attending weekly OT Cyber Security Solution meeting Attending weekly OT Leadership meeting Assessment\Scoping of Global Sector for each site located world wide OT Network Security Audit OT Network Security Remediation PepsiCo Sector\Site Assessment (Scoping) Tracker PepsiCo Master Sector \Site Tracker Knowledge on NIST 800-82, 800-53 and IEC 62443 IT Infrastructure Experience in Industries Hands-on experience on Windows environment, infrastructure Create\ Update Network Diagram using tools like Visio Interface with site\sector leads or third party collect information remotely based on defined checklist and process flow. Create Executive Summary Report (MS Word) as per pre-defined template and initiate approval process OT Cyber Security Basics NIST Guidelines on IC Security General Network and Firewall Rule Understanding Fast past on demand Priority based response for Scoping \ Assessment of Global Sector \ Local Site. Kforce at NTT DATA Infrastructure & Cloud Computing 9-17-2018-01-18-2019 Consulting | Digital| Managed Service | Industry Solutions Position: Security Transitions Specialists\Engineer Advisor Responsibilities: Hands on experience in Setup, Configuration, Validation, Verification and Final Test. Hands on experience Accessing jump Server. Hands on experience with the following: Qualys (Vulnerability) ,TACACS+CICSO ISE, Malware Bytes,(Anti-Virus) Workstation Agents, Checkpoint (Encryption) and PTC (Collector) like McAfee Nitro (SEIM). Hands on experience with Discovery of the following task within in the Project as follows: Console, Host Name\IP Address, Network Port Information, Physical Location of the Servers. Version Information, Release Information, License information, Policy Information, Use Case, Correlation Rules, Alerts\Triggers, Owner Information, Network Map Information, End of Life Information, and DR Information of the Platform or Device in Question. Task-by-Task Break Down to Do and To Get List. Hand of f and Turn over Documents. Pre-Go and Go-Live kick off

Major Projects. Attending daily, weekly, and monthly project team meetings. Working very close with PM on a Clients\Customer Projects. Documenting each dependency on each task of the project to PM. Timelines, Milestones are met in given time to complete the project. Working with other Team members. Working with info Sec-Transitions Tracking for recording Project Task progress. Working with Clients Application Portfolio Excel Spread Sheet. Attending daily. Weekly, monthly meeting. Creating Playbook\Run book per Device\Platform assigned for Project. Knowledge transfer to new PM on the Project and working with PMP & PM3 Concepts. Working Synergy SAP Project Time Tracking\ MYTE Time Tracking. Scheduling WebEx and Skype meeting as required. Product\Device\Platform from unmanaged\managed Client Admin Guide. Working knowledge of Automatic Script, Use Cases, and Correlation Rules. Alerts and Triggers depending on SOC Platform or Device. With Account Leadership and Transition Leadership. Purpose: Transition Status Update, Program Status, Tower Update, Milestones, RAID items, Actions, Executives Support and Charge Request. Vulnerability Assessment Analyst A Line Staffing for CVS Vulnerability Management Evidence Team July 2018 to September 2018 100% Remote Contract\Project) Hands on Trouble Shooting Evidence and Zero Day Process. Hands on experience working with Information Security in a large and complex enterprise network. Hands on experience working with Vulnerability Management team and various IT teams. Hands on experience working Qualys Scan Results. Collaborated daily with IT and business functions to understand vulnerabilities. Track evidence record submissions to closure or rejections process. Interfacing with Technical teams, i.e. Network, Firewall, platform (Windows/Unix). Coordinate updates to Vulnerability Management repository, Kenna to insure evidence related changes are made to VM records. Working knowledge of Networking fundamentals (all OSI layers) Hands on experience Qualys. Hands on experience with Vulnerability Management Hands on experience with basic scripting and Archer System Excellent communication skill , written and verbal Experience fostering and maintaining relationships with key stakeholders and business partners Hands on experience follow through next logical step to resolve issues Malware Analysis Working knowledge of Malware Reverse Engineering Working knowledge and understanding of

CVSS, CVE, CWE, CPE, CCE, CWE, OVAL, SCAP and other standards Working knowledge and understanding of (Windows, UNIX, Linux, and AIX, etc.) with emphasis on system hardening using vulnerability assessment. Tier Two Service onsite for Baker Botts, Dallas, Texas March 21- End date 4-12-2018 Information Security Analyst - Sec Ops Hands on experience Vulnerability Management (Nessus Tenable Security Center Vulnerability Scanner) Hands on experience for SIEM Alert (eSentire MDR) Hands on experience Security Event Log SSH logs and FTP logs. Hands on experience with Remediation of Alerts content within SSH logs and FTP logs. Hands on experience conducting Scans, generating reports and tracking remediation. Hands on experience working with i Manager File System. Working knowledge of DMS Document Management System. Hands on experience using Heat ITIL creating and assigning tickets. Hands on experience using AD to hunt, investigate SSH\FTP log information. Maintaining Security\Network Matrix Spread sheet. Hands on experience investigating, hunting for following information: Sources IP Address, Host Name, User Name, Protocol, Destination IP, and Action Request. Hands on experience and working knowledge of eSentire (Security Operation Team) working with Alerts, and Correlation Rules. Hands on experience using US Federal Agency CERT Incident Category: CAT5 Hands on experience and working Knowledge of McAfee Correlation Rules related to eSentire Alerts. Hands on experience and working Knowledge of White listing External IP Address External Source. Hands on experience reviewing eSentire (SIEM) Weekly Reports: Executive Trends, Qualified Threat, Executive Summary and External Concerns Weekly Reports. Malware Analysis Working knowledge of Malware Reverse Engineering Hands on experience working with PCI, and SOX. Attending Daily, Weekly and Monthly Staff team meeting. Completing all Task and Projects on time. Completing all mandatory internal info Sec training material. CSI-Cyber Security IAM Specialist Collabera onsite for BCBS - Richardson, TX September 2017 to March 2018 Information Security -Fulfillment Team Hands on experience RSA Secure Logon Server by EMC Corp version 8.1 SP 1 P 15 this is: A RSA Authentication Manager for granting end user Access for Secure Environment. Hands on experience and working knowledge of Identity, Authentication, Access, Reporting, RADIUS, and Administration. IAM day to day work flow. Granting Access to end user RSA Token Helper_v128 Automated Script Tool. Supporting and granting access to internal EU for Any Place, Any Place, VDI, Any Place VPN, Any Place Web, and Any Place off Shore. Supporting an NON-BYOD and BYOD mobility for RSA token for internal and external EU. Wyse Box EU (Thin Client) and granting access. Access Now Portal \Data Base build: 11.1.0-3 to find internal and external end users information and profiles. Microsoft 2010\2016 and O365. IBM\Lenovo hardware Think Center, Think Vision. Understanding HIPAA\PHI\PCI\and SPI. Service Now and Identity IQ by Sail Point\ITIL Process SGON granting Network Security Access to internal and External EU\ Image Application IBM Mainframe also known as OS\\390, 5655-A27. Adding EU profile, Updating profile, Granting EU profile, and Updating EU Access to Different Security Levels and Changing EU Access.\Manager Console. NetIQ Manager 2 version 2.7.7.4 Active Directory Congo's Administration following task: Finding internal\external EU, Delete, Add, Change and Move EU\Resting EU Password. Verifying approvals and exception before granting EU Network and Security Access of different Levels\ Top Secret Mainframe Request. With internal and external EU tasks as follows: Modify EU details, Modify Roles, View Authorities, and Activity Logs. Working knowledge of Exception, Approval Process, Change Management Process, Trouble Shooting, Escalation Request and Change Tickets. Using Identity IQ for finding internal and external end users profile And Network Access information and making sure process and steps are followed during on boarding process \ working multiple queues at same time and being team player. Training new team members on internal process, and applying security platforms and tools and brining them up to speed\ always eager to learn, apply, adapt to new Security Tool and Platform. Getting all task and projects done in a very timely manner. Hands on experience working in a very fast pace CSI Cyber Security-information Security -Fulfillment Team. Granting end users access to on DCUN with mainframe. Granting access to end users on BAE(Business Acquisition Alpha Code Platform). Granting Access to end users on WC3 Platform. Granting Access UR1s\UR2s in Top Secret Mainframe Area. Granting Access XGM Creation in Mainframe Platform and iManager 2 version 2.7.7.4 Platform. Terminating end users on multiple Mainframe Applications. Resolving (SNOW) Service Now tickets for multiple queue like: HCSC

IS Authorization Management Incidents: RSA Hard and Soft Token Incidents, Image Incidents, WC3 Incidents and XGM ID Incidents. DCUN mandatory training completed on time. DCUN is special Security Access within Mainframe for Vanguard Identity Management System Network Sr. Analyst-NE , Digital Identity Services Kfroce ,inc at NTT Data July 2017 to September 2017 Supporting Service Now Dell Service Management Suite Supporting BMC Remedy User Hands on experience Microsoft Visio 2013 and Microsoft Project 2013. Supporting the following platform Source fire, Blue Coat, and RSA\Radius. Hands on experience working with McAfee Nitro, Symantec AV and Fire Eye. Hands on experience working with Project Managers and Enterprise Transition team. Hands on experience working with Microsoft SharePoint. Hands on experience working with Digital Identity Service and Security Transitions Team. Attending Daily, Weekly and Monthly project status team meeting. Bi-weekly 1-on-1 project meetings. Bi-weekly Knowledge transfer WK DR Project meetings. Completed mandatory NTT Data SOM Service Now training. Completed mandatory NTT Data OPAS v2 training. Completed mandatory NTT Data PMO & PM3 training. Achieved & Earned PM3 Level 1 internal Certification for NTT Data's Project, Program, & Portfolio Management Framework. McAfee Nitro Task-by-Task Break Down To Do and To Get List. Working knowledge of McAfee Nitro Production Environment. Symantec A\V Task-by-Task Break Down To Do and To Get List. Working Knowledge of Symantec A\V Production Environment. Now I am taking ownership of Cisco Source Fire, Symantec Blue Coat, and RSA. I will be responsible for Installing , configuring and setup Cisco Source Fire, Symantec Blue Coat and RSA on WK DR Site. By following WK DR Project Plan and Schedule. Cisco Source Fire Task-by-Task Break Down To Do and To Get List. Working knowledge of Cisco Source Fire Production Environment Symantec Blue Coat Task-by-Task Break Down To Do and To Get List. Working knowledge of Symantec Blue Coat Production Environment RSA\Radius Task-by-Task Break Down To Do and To Get List. Working knowledge of Symantec RSA\Radius Production Environment Completed Mandatory training session for Exception Letter Education Awareness Effort. Attending Bi-weekly for NTT Data Project Team, Account Leadership and Transition Leadership Purpose: Transition status update, Program status, Tower Update, Milestones, RAID items, actions, Executives support, and charge request. Attending weekly Brown Bag Knowledge Transfer training for IPS\IDS Appliance. Working with Enterprise Team member. Information Technology Security Specialist GMC Technologies, Inc at VB Advisors March 2017 to July 2017 Supporting Nextiva VOIP Phones Supporting Nextiva Switch\Router Supporting End User IPhone and Android for O365 Configuration. Supporting 0365 on End User Desktops. Supporting Wireless Networking Device LinkSys EA2700. Supporting Uni Fi UBIQUITI Wireless Network Device AP AC PRO Supporting following Network HP Printer. Printer Color LaserJet MFP476NW,HP Office jet Pro 8600 Plus & HP Color Laser Jet CP3535n. Supporting Day Trader Desk configuration for video display. Supporting Dell and HP Monitor Day Trader Configuration. Working with vendors like Go Daddy and Nextiva. Maintaining SLA at all times. White Glove Customer Service Approach. Hands on experience imaging Desktops and creating end user profile. Supporting Bloomberg Keyboard Technology. Supporting Anti- Virus Software and Node Security. Network Sr. Security Analyst Apex System Inc, at NTT DATA Operation\ Client NMG July 2016 to March 2017 Hands on Experience SPLUNK SEIM solutions and as mentioned below. Supporting large 5800 node distributed\cluster environment this first phase. Supporting 4 search heads, 7 indexers, and 100+ forwarders. Supporting Linux based environments. Providing outstanding customer service to NTT Data Customers. Coordinating escalations collaborate with technology teams to resolves all issues in timely manner. Perform other duties as assigned Perform system maintenance and maintain current documentation and propose process and technical improvement to management Management processes are followed and all incidents and requests are addressed within the required time to adhere to publish SLAs. Interim Team Lead over 14 Network Sr. Security Analyst. Creation, Deployment, configuration and maintenance of Splunk Dashboards. Creating Splunk Reports, Alerts and Searches. ITIL process and creating documentations. Malware Analysis Working knowledge of Malware Reverse Engineering Teaching training Splunk as SIEM. Extensive knowledge of logging methodologies. Supporting other Sec Ops products and Platforms to come. Service Now Rapid 7 Nexpose Vulnerabilities Scan on Pre Prod\ Prod assets SCCM McAfee ePO and its logs. VPN connection for NMG project. Change, Incident and Problem Management. Security Engineer TEKsystems at NationStar Mortgage December 2015 to July 2016 Chosen to be Co-Solution Architect for Implementing and deploying Splunk Creating PPT and Training material to Implement and Deploy Splunk Hands on experience running Pro Prod Scan on VM, Template, Physical and Blade Servers Hands on experience working with Service Account and CMDB on AD,elQ Network Secure Vue (SIEM),DAT Compliance McAfee Scans, Palo Alto (PAN) Web Contact Filtering Working on project for cleaning and purging 1507 service accounts records associated with AD and CMDB records Hands on experience with Entrust Identity Guard Admin Data Base creating new user requests Hands on experience working with Security Incident tickets for Info Sec group, Foot Print, Archer Exception process, creating Special Admin AD Group Hands on experience working with RSA Archer GRC Platform and Tasks mentioned below. SCCM. CVE, DSA,OVAL,RHSA,BID,IAVM and XF reports. Rapid 7 Nexpose Vulnerabilities Scan on Pre Prod\ Prod assets OKTA, ISIM, Workday process flow for new end users RSA token\Entrust - Identity Guard\ 2 Factor Authentication VPN connection and RSA token. Malware Analysis Working knowledge of Malware Reverse Engineering Enterprise Change, Incident and Problem Management Remote Technical Support Specialist CBS Central Business Solutions Inc. at Avanade\Accenture\Microsoft October 2015 to December 2015 contract\project) Supporting Microsoft Office 365, Microsoft Exchange, Lync, Share Point Supporting and configuration clients emails of Microsoft 365 Analyzing and providing feedback on the development process Supporting AD and Advance Software, Hardware , Network , Security related Trouble-shooting Lead Technical Support Hardware\Software\Network Specialists Thumbtack.com September 2015 to October 2015 Advance troubleshooting, virus Removal, Backup and Restore Support and On-site Service Supporting HP, Dell, Okidata, Lexmark laser printer, Wireless Technology, Encryption Technology, MAC OS, Asset Management and Thin Client, Laptops, Desktops, workstation and Servers Technical Support Specialist II Information Technology Apex System Inc, at Parkland August 2015 to September 2015 Installing, configuring, troubleshooting and maintaining the Microsoft Windows 7/8 OS Supporting VDI, EPIC System, Browser Support, Network Access and

AD HEAT ITSM incident workflow process and Supporting Citrix Applications backend support. Network Configuration of Zebra Printers and Device name or IP Address via web connection Working with Lexmark Printer testing them via web connection Tricerat Simplify Console Enterprise Management Implement and maintain information security policies and procedures Working knowledge of TCP/IP and related network services (i.e. DNS. SMTP, DHCP, etc.) Hands on experience on S Hands on experience working with Service Account and CMDB on AD, eIQ Network Secure Vue (SIEM),DAT Compliance McAfee Scans, Palo Alto (PAN) Web Contact Filtering CCM. Working knowledge of Fire Eye. Thorough understanding of security, network architectures and protocols. Technical Support - IT\IS Technical Trainer A Critical Path Inc - Dallas, TX March 2015 to July 2015 Key Achievement, pursuing: CompTIA CASP (CompTIA Advance Security Practitioner) Hands on Experience teaching participants: CompTIA 220-801 PC Hardware\ Networking \ Laptops \Printers\ Operational Procedures Hands on Experience teaching participants: CompTIA 220-802 Operating Systems\ Security \ Node-End Host Encryption Technology\ Virus Definition File \ Wireless Technology\ Mobile Devices \ Physical Security Technology \ Troubleshooting Senior IT\IS Technical Trainer MNK Infotech Inc - Dallas, TX January 2015 to March 2015 Part of DCCC, CCCC, and TCCC Information Technology system Following information Technology courses MCSE\MCA\MTA Information Technology Infrastructure Library (ITIL) Foundation Understand IT Service management as a practice Information Security web based programs Symmetric encryption and Public-Key Infrastructure (PKI) Secure programming techniques Threats\Worms\Malware\Spyware \Virus\Trojans Define threat modeling Describe authentication, authorization, access control, confidentially, data integrity, and non-repudiation Sr. Information Technology Network Filed Engineer\Tech On Force USA Inc - Dallas, TX December 2014 to February 2015 Advance Diagnostics, Trouble Shooting, Encryption and Anti-Virus Technology. Information Technology Network Access Administrator ClubCorp USA Inc - Dallas, TX October 2014 to December 2014 Working closely with SOX compliance as SAR team member Following the correct Security Protocol before granting end users Network Access Granting Access to End Users to Internal and External OEM based Application Working with Active

Directory and Processing Every Day Oracle Termination Report. Working with RSA and VPN protocols and security and Manage Engine Service Desk Plus Worked with F5 load balancer and granting network access Hands on experience Enterprise Change, Incident and Problem Management Thorough understanding of security, network architectures and protocols. Hands on experience working with Service Account and CMDB on AD, DAT Compliance McAfee Scans, Palo Alto (PAN) Web Contact Filtering Senior Operation Application Support Specialist Fiserv, Inc - Dallas, TX May 2013 to October 2014 Security Responsible for Security, Networking, Advance Trouble Shooting and Diagnostics Understanding of, or experience with PCI DSS compliance requirements Server side Using graphs, dashboards and Queue monitors and alerts traps to fix file related problems Responsible for Monitoring and troubleshooting issues Assign assignment task and opening and closing CRQ\RFC\COB Using the ITIL process and methods working with all changes made for Business Unit. Running Scripts to Automate Batch File process Hands on experience using below mentioned tools and technology at Enterprise level Beta Test Splunk on production Servers Hands on experience working with SQL Server with Application Support Hands on experience working Qualyguard alerts on Enterprise level on production servers, Critical Watch alert and in house Auditing tools and Utility Tools. Hands on experience supporting Citrix Application and back end back end support. Hands on experience of understanding usage of Wireshark on production servers Responsible for Network administration, vulnerability assessment and various security related vulnerabilities and resolutions. Hands on experience fail over testing, disaster recovery testing and other readiness efforts. Hands on experience using below mentioned tools and technologies: CA Sterling Control Center Console 5.2.06, Clarity Project\ Incident Management Process, BMC Remedy Knowledge Management version 7.5, Power Grep by Great Software Cot. Ltd, Bare Tail Pro by Baremetalsoft, Major Event Notification Process, Incident response, working with patch management team, Speech Recognition Licenses Tool, CA Technologies Intro scope, CA Technologies APM Cloud Monitor, Command Center Zone 2 Drive Checker Tool, CA Workload Control Center, Payment IVRS and Testing Payments IVR, SCCM\Voice Object Restart Patch Updates. PC LAN TECH\ Security Administrator Express Scripts, Inc - Fort Worth, TX July 2009 to May 2013 Supporting 250 End Users onsite \150 End user Off Site \ 25 Pharmacy Tech at home Hands on Experience Assets management technology, ITIL process, policies and procedures. Working with HIPAA process, guide lines, producers and rules as Information Technology Professional was HIPAA certified eternally with Express Scripts fortune 1000 companies of America Imaging Windows 7 on Laptops, Desktops and Thin Clients Understanding of Hard Drive Encryption\Decryption Technology, Anti-Virus Technologies Hands on experience using authentication and authorization process on production network Endpoint Antivirus migration, upgrades, and deployment Hands on experience on large migration , upgrades and deployment work flow process Hands on experience of Disaster Recovery Plan and yearly DRP exercise, Scanning Physical site of rouge wireless devices, physical security hardware and software, VOIP phones and VDI technology Citrix Application Wise Thin Clients, Conference Video Hardware and Software, PII and PKI technologies, McAfee ePO Policy, E-Policy 60 day report of false positives and false negative report Performed troubleshooting, configuration, administration and management of Thin Client Technology (Virtual Farm) at AD level, and Regular scans for Nodes on Network Troubleshooting, configuration, administration, management of RSA\VPN\Citrix Hands on experience fail over testing, disaster recovery testing and other readiness efforts. Hands on experience change management utilizing documented procedures. Thorough understanding of security, network architectures and protocols. Reference will provide upon Request Skills SECURITY, SPLUNK, TRIPWIRE, VPN, WIRESHARK, EXCHANGE, NETWORKING, REMEDY, TCP/IP, FIREWALL, GHOST, RSA, CITRIX, LAN MANAGER, TACACS, TCP, INTERNET EXPLORER, ETHERNET, WIRELESS, LINUX Additional Information TECHNICAL PROFICIENCIES: Software/Database: MS Office 2007/2003/XP/2000,O365, Internet Explorer, Firefox, , Chrome, Remedy, Service Now, Foot Print, Norton, McAfee Antivirus/ Security, Entrust, Spyware-Adware products, and other OEM products Operating Systems: Windows 3.1, 9x, Windows NT, Windows 2000, MS Exchange, Windows 7,Windows 8, Windows Vista, Windows XP, Windows 2000 Server & Workstation, Mainframe, Mac OS. Windows 10, Microsoft Office 365 Hardware: Dell Hardware Platform, HP\Compaq hardware Platform, IBM\Lenovo Platform, Native

Networking: LAN\WAN, VPN, Wireless, TCP/IP, Novell, OS2, 100Base-T, Ethernet, Secure ID, Citrix, Linux Hardware Server Support, Dell Sonic Wall VPN, Tools: LAN Manager, Firewall, Norton Firewall, Ghost, McAfee/Norton Antivirus Protection Utilities, Defender Soft token Response, New Tools used: McAfee ePo, McAfee Nitro, Symantec A\V, Archer GRC Platform, Entrust Identity Guard , Service Account Data base, CMDB, Web Sense, Bit locker (MBAM), TACACS, RSA envision, Source fire, QualyWAS, tipping point,Veracode, WhiteHat, Critical watch. Beta Tested on Production Servers: Tripwire, Splunk, Wireshark, and Critical Watch HP Tools: HP Firmware, Smart Start, ILO, HP Hardware Server Management Working Knowledge ISIM, OKAT, Workday, I AM Support, Nextiva, PM3, PMO, OPAs v2, SOM Automated Scripts, Veracode, WhiteHat Fire Eye, Cloud and AWS.

Name: Kenneth Sanchez

Email: stacyherrera@example.net

Phone: 994-259-2029x54753