Security Analyst Security Analyst Cloud Security Engineer Kyle, TX A well-qualified and results-oriented InfoSec professional adept at analyzing existing infrastructures and developing solutions to meet organizational needs. This includes documenting and updating policies and procedures to align with industry best-practices, consolidating physical resources into virtual or cloud environments, and managing hybrid environments. Knowledgeable in performing vulnerability assessments for existing infrastructures, analyzing security gaps and logs, creating remediation reports, analyzing internal security gaps, and assessing 3rd party tools for organizational use. Work Experience Security Analyst ClearData - Austin, TX August 2018 to Present Investigate alerts and suspicious activity, analyze log files for attacker information and correlating evidence, provide insight to compliance concerns and approve or deny customer requests based on HIPAA and HITRUST requirements for AWS, Azure, and GCP cloud environments as well as some legacy VMWare datacenters for this startup. Selected Contributions: Monitor ticket queue that collects all alerts and events from security appliances monitoring and protecting customer environments, then generates tickets based on notifications received. Tickets are also generated through customer and employee requests to the security operations team for changes or compliance artifact evidence gathering. Conducted interviews to fill positions for on-shore and off-shore roles for the security operations team involving organizational transformation to 24/7 support. Contributed to team development of training documentation and hosting virtual meetings to discuss training plans for the new roles to transition into. Created or edited SOP documents in Atlassian knowledge bases involving gathering evidence for incident response evidence gathering, AWS monitoring and NACL adjustment, vulnerability scanning and management procedures, Alert Logic notification responses and analysis for multi-tenant environments, and documenting analyst tools with access and use procedures. Created a daily checklist for analysts to review, document, and action on any changes or alerts to the internal ClearDATA environment, including physical access log reviews, tool maintenance and licensing reviews, escalating internal AV alerts to IT for remediation or IDS/IPS alerts to networking, terminating former employee access. Contributed to team development of a documentation request process. Created peer-review process to ensure that created documentation

is reviewed and approved by another team member before being put into production to reduce errors and evaluate the usefulness of the document, then provide feedback until the document is approved for production use and new Standard Operating Procedures are adopted. Developed Python scripts for processing Salesforce tickets with known responses to filter out noise tickets and focus on more serious customer concerns, resulting in saving hundreds of hours from manual processing a month. Contributed to the team development of an internal Tenable API tool that is used to automate vulnerability scan reports for customers, again reducing the manual workload for current analysts while providing an on-demand service for customers. Contributed to internal risk analysis for ClearDATA with the rest of the security team by performing benchmarking exercises using the CIS framework, identifying existing security gaps through multiple cross-functional meetings, and making recommendations or implementing changes to assist. Remediated CIS benchmark findings and created SOPs and evidence for log management, deploying SIEM and/or log analytic tools, and regularly reviewing logs. Perform analysis of packet captures (PCAP) flagged by IDS/IPS tools for review using Wireshark and/or tcpdump to look at packet details and analyze payloads at a granular level for suspicious activity, send/receive data, session information, TCP flags for socket creation, gathering SQLi or other malicious input evidence, decoding strings to more human readable formats, and creating reports with evidence and any further remediation steps that the customer or another co-worker would be responsible for. Participated in planning, deployment, troubleshooting, administration, and documentation of SIEM tools used to monitor the internal environment and aggregate logs from identified critical sources Deployed IDS appliances, log and threat management instances, vulnerability scanner nodes, and endpoint protection agents that reported back to SaaS security solutions. Identified solutions using these tools to forward data into SIEM for alert and log ingestion. Identified security gaps and developed presentations for leadership teams to notify them of the problem and provide recommendations for remediation steps or to vendors who could supply a solution that fit our requirements. Presented these options before purchasing committees and provided evidence for research and comparison of other vendors to support why a specific tool was identified. Perform initial review of customer environment change

requests and ensure that the ask contains appropriate information necessary for review before escalating to engineers for implementation. Performs QA checks after changes have been implemented and notifies customer of changes and confirms resolution. Create Python scripts using different AWS-friendly libraries like Boto3 to perform DynamoDB queries, assume roles through STS, gather instance information from EC2 assets, and other tasks in need of automation. IT Helpdesk Technician/ IT Security Analyst Professional Contractor Services Incorporated - Austin, TX April 2016 to August 2018 Provided remote support to several jobsites and users across the US, including issues with workstations, WAN connections, firewalls, servers, VOIP systems, VMware hosts and guests, and hybrid infrastructures. Wrote policy and procedure documentation to fulfill compliance standards covering subjects such as hardware life-cycle maintenance, creating/managing/removing user accounts, tracking and documenting assets, deploying security awareness training campaigns, and other documentation as needed. I work with a variety of vendors and test software and hardware products for compatibility and ease of use for non-technical employees as well. Selected Contributions Developed asset and user account lifecycle management documentation for ISO 27001 and DHS required standards including onboarding and terminating employee access, new asset onboarding, tagging and tracking requirements, and securely decommissioning hardware for retired assets. Managed identity/access controls for physical access to facilities including multi-factor authentication badge access. Developed and documented procedures for creating new users and terminating revoked access to facilities, collecting employee files from workstations and Office 365, and sanitation procedures for used workstations to be re-deployed. Administered bi-weekly phishing simulation attacks and monitored ongoing reports as part of a security awareness training program. This program led to a significant reduction in the percentage of employees falling victim to social engineering attacks, showing the training program was successful. IT Department Representative for the DSS Insider Threat Program, developed an employee-focused web-based reporting tool for insider threat alerts. The development of this tool was key to meeting DSS Insider Threat Reporting compliance requirements. Systems Administrator St. Andrew's Episcopal School - Austin, TX July 2013 to

March 2016 As a Systems Administrator, I managed Active Directory group policies and accounts, installed networked Ricoh printers, managed file/print servers, Windows Update servers, and developed Windows Deployment Services for re-imaging corrupted student and teacher laptops. I supported a high school One to One laptop program for 650+ laptops; served as the liaison for warranty repairs; and employed a local, web-based ticketing system to manage workloads. I also supported the rollout of a web-based teacher/student/parent communication system and was a point of contact for troubleshooting/account management for the program. Selected Contributions: Transitioned teachers, staff, and students with required laptops from on-premise email and file storage services for to an Office 365-hybrid environment as part of a long-term cloud migration strategy. Reduced expensive licensing and hardware costs associated with reimaging systems by using a combination of open-source tools, Microsoft Deployment Toolkit, and Windows Deployment Service with existing assets to deploy updated images over PXE boot to wipe and restore infected systems, reducing the former associated hardware, software, and licensing of the previous imaging process to zero. Migrated critical infrastructure services from multiple physical hosts to virtualized instances in a single IT closet, reducing hardware and utility costs. IT Support Contractor - MRSW Management LLC, PDS Tech Austin Energy - Austin, TX February 2010 to July 2013 Ensured system security/stability by creating scheduled maintenance routines to provide updates; tested migrations for Windows OS; and employed Windows Deployment Service and Microsoft Deployment Toolkit to build custom images and automate deployments across the LAN. Selected Contributions: Created VMs in Windows Server 2008 R2 using Hyper-V to create baseline system images compliant with NERC/FERC regulations as City of Austin Policies/Standards. Supported Marketing's Mac OS X environment, including a backup and software deployment server for reimaging systems. Provided desk-side and remote support for 800+ users across 5 jobsites in the Austin area. Coordinated the Windows XP to Windows 7 migrations with multiple departments to ensure that the migration and corresponding updates completed successfully while minimizing business process impact. Education Masters of Science in Information Assurance and Security Capella University - Minneapolis, MN 2016 Bachelor's in Science Texas A&M University -

College Station, TX August 2004 to December 2009 Skills LAN/WAN Troubleshooting (5 years), Firewall/IPS Administration (2 years), Asset Management (5 years), Policy Development (2 years), Patch/Software Management (4 years), Cloud Computing (3 years), Security Control Administration (2 years), VMWare/Hyper-V Administration (5 years), VPN (2 years), Event Log Analysis (3 years), NIST Cyber Security Framework (Less than 1 year), PCI DSS documentation (Less than 1 year), ISO 27001 documentation (Less than 1 year), Off-Site Backup Management (2 years), Windows Server (4 years), Nmap (1 year), Metasploit Framework (Less than 1 year), Python (1 year), Powershell (1 year), Wireshark / Packet Analysis (2 years), OpenVAS (1 year), Nessus (2 years), Cyber Security (6 years), Amazon Web Services (AWS) (1 year), IDS/IPS Traffic Log Analysis (1 year), Tenable Administration (1 year), Linux (1 year), Active Directory, Security, CIS (Less than 1 year), Alert Logic (1 year), Trend Micro DSM (1 year), LogRhythm (Less than 1 year), Elasticstack (Less than 1 year), SIEM (Less than 1 year) Links https://www.linkedin.com/in/sumner072 Certifications/Licenses CompTIA A+ March 2016 to March 2019 Code: 3ZBH2PCGECF1Q87Z Verify at: http://verify.CompTIA.org CompTIA Security+ March 2016 to March 2019 Code: VBEPJ91G3LB12P51 Verify at: http://verify.CompTIA.org Junior Penetration Tester September 2015 to Present Certificate ID: EJPT-100569 Certified Information Systems Security Professional (CISSP) June 2017 to June 2020 ID # 612374 A valid IT Specialist certification Assessments Technical Support Highly Proficient May 2019 Measures a candidate's ability to apply protocols to identify errors and solutions in order to maintain system function. Full results: https://share.indeedassessments.com/share_assignment/7sy9iwqabqgiadxl Email Expert May 2019 Measures a candidate s ability to effectively compose and organize email messages. Full results: https://share.indeedassessments.com/share_assignment/s3w6nmhwic5u9v7q Research Highly Proficient May 2019 Measures a candidate s ability to follow protocols, interpret statistics and graphs, identify errors, and choose research methodology. Full results: https://share.indeedassessments.com/share_assignment/i0weitsejt84gwek Critical Thinking Expert May 2019 Using logic to solve problems. Full results: https://share.indeedassessments.com/share_assignment/7s2noedgd033vtc9 Data Analysis Expert

May 2019 Measures a candidate's skill in interpreting and producing graphs, identifying trends, and drawing justifiable conclusions from data. Full results: https://share.indeedassessments.com/share_assignment/t4kmfc2prwx79xz4 Teamwork: Interpersonal Skills Expert May 2019 Resolving disputes, solving team problems, and understanding nonverbal cues. Full results: https://share.indeedassessments.com/share_assignment/txcwm-thqvp-y6ue Data Entry Expert May 2019 Measures a candidate's ability to accurately input data and effectively manage databases. Full results: https://share.indeedassessments.com/share_assignment/y99ompk-slfu58qy Indeed Assessments provides skills tests that are not indicative of a license or certification, or continued development in any professional field.

Name: Kenneth Guerrero

Email: erica41@example.com

Phone: +1-358-703-5814x14968