Linux Systems Engineer Linux Systems Engineer Deployment Engineer - Diligent Consulting San Antonio, TX A focused, team-oriented engineer with a knack for automation. I have 5 years of hands-on experience supporting, automating and optimizing mission critical deployments. Leveraging cloud based solutions is my main focus. Security+, CySA+ and CSAP certified. Github Page: https://github.com/Dmwatts79 Work Experience Linux Systems Engineer TrueAbility - San Antonio, TX Present Current tasks include being responsible for creating docker images using docker-compose. Creating, monitoring and maintaining BASH scripts to ensure that provisioning for end-user will complete as expected. Testing various scripts in a test environment before pushing to production. Ensuring that AWS and GCP network traffic is being logged and tagged for parsing. Assisting build scalable, resilient AWS EC2 infrastructure by leveraging AWS auto-scaling. Understanding various Linux distros such as Ubuntu,CentOS, Redhat & OpenSUSE. Utilizing Jira, trello and GitHub for change management and version control. Systems Administrator Diligent Consulting - San Antonio, TX June 2018 to July 2019 Implemented a security monitoring system for over 200 hosts Managed Windows 2008, 2012, 2016 and Linux based servers (total +- 50) Use various tools including Nessus, OpenVAS & Burp suite for security testing Utilizing power-shell scripts to manage Office 365/ Active Directory sync with Azure. Managed IAM roles within AWS Cloud environment Manage docker based images Created/Manage test vagrant images. Working experience securing servers based on STIG's Familiar with frameworks such as PCI-DSS and NIST ? Manage vulnerability program to assess various servers, services and web applications utilized OWASP and ZWAP for web application vulnerability assessments ? Implemented a BYOD (Bring Your Own Device) security policy ? Managed patches via a identical test environment ? Presented risk reports based on industry findings ? Maintain various snapshots for virtual environments including vSphere/VMware ? Managed the procurement and deployment of various endpoints. Junior Systems Administrator (SOC Environment) Daemon Systems - San Antonio, TX November 2015 to August 2018 Renegotiated a new contract with SIEM provider to save 66% total cost per month (Over 45k per year savings) Interacted with wire-shark, Nmap and OpenVAS for vulnerability testing ? Acted as the POC for all customers in regards to network upgrades, contract dealing and SLA requirements. (roughly 50 customers) ? Maintained Domain Controller servers for over 50 customers. ? Maintained Fileserver environments ? Implemented remote security access systems (RAS) using cisco VPN routers ? Engaged, tested and quantified user awareness by conducting email phishing campaigns ? Utilized both auto-task and Salesforce CRM as a platform to track and quantify ticket metrics Desktop Analyst I (SOC Environment) ? Manage all level I and II helpdesk tickets (50-75 tickets per day) ? Managing the add and removal of users from active directory Education BAAS in Information Security & Assurance Texas A&M San Antonio December 2019 AAS in Information Security & Assurance San Antonio College September 2017 Skills SIEM (2 years), Cisco, Sharepoint, NIST (2 years), PCI-DSS (2 years), Windows Server (5 years), Programming (2 years), Python (2 years), Bash (2 years), Powershell (1 year), Barracuda Backup (3 years), ArcServe (3 years), Solarwinds (2 years), Networking (5 years), Vulnerability Scanning (3 years), Git (1 year), Ubuntu (2 years), Fedora (2 years), Red Hat Enterprise Linux (1 year), Arch Linux (1 year), Vulnerability Management (3 years), Active Directory, Microsoft Office, testing, training, security Certifications/Licenses Security+ Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents not just identify them. CySA+ (Cyber Security Analyst) Present CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. CSAP (Certified Security Analytics Professional) Present Groups Board Representative Alamo ISSA Present Assisting with the recruitment of teachers for CyberPatriot for high school students Responsible for vendor relations of Alamo ISSA Infragard Member Present A partnership between multiple big businesses and the FBI. We get private national security concerns that can be translated to warn organizations before public knowledge. Additional Information I am currently learning more BASH scripting and will be continuing on to learn about ansible and chef and Jenkins. I hope in the next 12 months to gain a proficient understanding of low level exploitation using the C programming language.

Name: Penny Cruz

Email: vargasraven@example.org

Phone: 350.283.4766