IAM Security Analyst/Engineer IAM Security Analyst/Engineer Fort Vancouver, WA Authorized to work in the US for any employer Work Experience IAM Security Analyst/Engineer Tek Systems-Nike - Beaverton, OR December 2018 to Present Advanced Powershell Scripting for data analytics and correlation with AD and Sailpoint IAM System. Troubleshoot Locked out issues in Okta and AD. Configure MFA for end users : Call, SMS and Google auth code generation. SailPoint :Troubleshoot IIQ identities, correlation of ID lockers, entitlement group configuration, Bulk changes. Write Standard Operating Procedures documents for fixing issues consistently and standardize processes. Processed. Daily termination and audit reconciliations. Investigated Locked out incidents with DEVO (Data Analytics Tool). Currently enrolled in a Python scripting class on line. IT Security Administrator Conmet - Vancouver, WA February 2017 to October 2018 Designed and implemented automation processes for user account life cycle (Creation, terminations, changes, transfers, entitlement reviews and revocation schedules). Advanced Powershell Scripting for interconnecting applications with Active Directory. Utilization of APIs in scripting using restful Responsible for the User Lifecycle and identity access management. New account creation, changes, transfers and terminations for users in China, Mexico and the USA. Identified data owners and created a data ownership matrix with the purpose of biannual entitlement reviews and internal audits. Scripted data ownership matrix maintenance into AD groups and data ownership matrix report. Handled 3000 service requests via Cherwell ticket system during FY 2018. That included 650 New account creations with their respective approved access, changes, terminations, new server shares, VPN troubleshooting and provisioning, monthly contractor reviews, lastlogontimestamp user reviews to identify stale accounts, conference room creation requests, service account requests, script creation requests, etc. Provided support for 18 locations in the USA, 3 in China and the Mexico facility. Expedited Cyber Security News Letter in Spanish, English and Chinese every month. Conducted biannual phishing campaign using Wombat Technologies for China, USA and Mexico. Automated user account creation, termination, changes and AD account reporting via PowerShell scripting. Process Improvement: Reduced time in account creation process dramatically by eliminating manual processes, setting up baselines for access. Approval

access for new accounts were scandalized with a data ownership matrix in which managers approved with one single reply reducing the number of emails per approvals. Created access profiles for summer interns and contractors which were set to be validated by the Engineering data owners. Reduce cost on paper by providing level access reviews that presented the data structure, level access, groups involved and members within each group reducing complexity for data owners. Maintained Sophos MDM user database, expedited required actions upon user terminations. Utilized Splunk for log correlation for user account investigations. Used Proofpoint to managed email gateway protection rules against spam and in response to incidents reported. Conducted vulnerability scans against new implementations and worked with other teams to mitigate vulnerabilities. Created reports with Lansweeper to improve visibility on assets, location, encryption status, software updates and user correlation. Created audit reports and alerts on monitored security groups to monitor file server and active directory changes. Change alerts of interest were: deletion of logs, elevated privileges to Domain Admins, Enterprise Admins groups or any other group that is subject to the biannual audits. Reduced ticket volume and after hour calls on password resets by implementing a Manage Engine Self-Service Password with the password notification feature only. IT Security Administrator The Greenbrier Companies - Lake Oswego, OR Provided Desktop support at a senior level for 1 year then got promoted to Security Administrator reporting to the vice-president of IT. Provided corporate training and support in the USA and Mexico where travel was required Active directory management for 1700+ users with 48 locations in the USA and Mexico Troubleshoot Dell desktop and laptops issues. Restored OS and data accordingly. Modify users in AD according to Manager s request for permission access. Manage life cycle form for AD accounts. Schedule meeting with vendors for finding sound solutions to current security related issues. Create processes for permissions, access related to SOX and SAS70 compliance. Create business unit sites in SharePoint 2010 and managed access. Troubleshoot issues related to Postini (email gateway), email forwarding and delegation. Manage 300+ contractor AD accounts which require periodic renewal per corporate policy. Create corporate policy for various processes for SOX compliance purposes. Provide extensive report on AD

accounts for periodic audits. Saved Greenbrier 50k + by producing internal training materials in English and Spanish. Used and administrated Data Governance and Audit tools and technologies for audits such as Stealthbits, Varonis data advantage, Varonis Data Privilege and Data Classification. Saved Greenbrier 150k+ in salaries for a second Security Administrator by developing and automating processes with advance PowerShell scripting. Brought AD account audit from fail to an outstanding level in 12 months with a 90% overall improvement. Participated in the initial steps for IAM implementation, working with Dell Education Bachelor's in Applied Technology with emphasis in Data Network and Telecommunications EWU - Vancouver, WA January 2005 to June 2007 Skills Active Directory, Identity Access Management, Bilingual, Spanish Technology, User Life Cycle Management, IAM, Spanish Training, Bilingual Support, Security, access

Name: Jennifer Brown

Email: smitherin@example.net

Phone: 738.662.0862x50457