Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst Cedar Park, TX Experienced and talented cyber security IT professional. Manages IT security, IT risk, security compliance (e.g., data systems, network and/or web, applications, and within Vendor Management Program) across the enterprise by creating security policies, designing and executing vulnerability assessments, penetration tests and security audits and by ensuring enforcement of enterprise security documents. Additionally, is charged with ensuring procedures and activities comply with all regulatory requirements and internal policies, procedures, guidelines and standards. Authorized to work in the US for any employer Work Experience Senior IT Security Analyst Amplify Credit Union - Austin, TX September 2016 to Present Responsible for assessing information risk and facilitating remediation of identified vulnerabilities for IT security and IT risk across the enterprise and with vendors. Maintains the security plan to ensure the proactive security posture of the credit union along with establishing the security department budget Performs security management as the sole security person at the company Develops policies, procedures and standards that meet existing and newly developed policy and regulatory requirements including NIST, PCI, and/or FFIEC guidance. Serving as the expert providing the latest trends required by governing authorities maintaining compliance Develops internal architectural designs according to business needs and best practice following COBIT/NIST as a baseline Ensures the confidentiality, integrity and availability of the data residing on or transmitted to/from/through enterprise workstations, servers and other systems and in databases and other data repositories. Creates and maintains the portions of the enterprise's Business Continuity Plan and Disaster Recovery Plan related to area of responsibility. Ensures annual reviews of documentation library items are current and follows up with business units for completion of their required actions. Maintains and oversees the annual periodic security assessments by 3rd party vendors for evidence or vulnerabilities or compromise in the environment Member of the Audit committee and participates in preparations for security reviews and audit Implements security related monitoring and prevention tools Works with the IT team to ensure efforts are aligned and coordinated for vulnerabilities and risk Effectively responds to security audits from customers and other outside parties Manages and assists in performing on-going security monitoring of information systems including assessing information security risk through qualitative risk analysis on a regular basis and conducting functional and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements. Evaluates and recommends new information security technologies and counter-measures to senior management along with maintaining a strong security posture against threats to information or privacy, and develops security reports and dashboards User Account Creation Representative Capgemini - Austin, TX July 2015 to August 2016 Responsible for creation of user accounts in the corporate network using windows active directory win 2008-2013 Provides account creation for over 1000+ user accounts in the State of Georgia in active directory providing quality customer support Team member of 5 team UAR providing service desk and customer consultant services by creating user accounts, deactivations and adding permissions for share point sites Determines account permissions on accounts created and disabled across the State of Georgia thereby ensuring strict security preventing unauthorized access Created training package allowing new employees incoming to learn and perform duties for the position providing a faster ramp up speed on the how to's for the role Information Technology Coordinator/Infrastructure Mgr HCL America - Dallas, TX September 2006 to October 2014 Primary point of contact for overall IT responsibilities including day to day network operations management and systems analysis, system security management along with deployment of eight servers at the energy sector Sandow Power Plant. Various systems and backups, RFID systems, security and bandwidth management at power plant and surface mining company, also responsible for the mini-NOC where the servers, switches, APC units and Voip phone hardware is stored in the MER. Maintained over 20 MER equipment rooms with switch racks and cooling. Responsible for the installation of over 400 Cisco VoIP phones for plant phone upgrade. Provides project management and vendor oversight for network cabling/fiber installations/HVAC along with standard systems architecture (SSA), disaster recovery, access control and physical security in cyber security for prevention of unauthorized access into plant control systems providing NERC/CIP compliance following NIST/ISO compliance. Maintained the SCADA diagrams to ensure point of failure did not occur ensuring uptime was maintained Performance driven subject matter expert (SME) providing IT infrastructure security management consultation and analysis of the organizations business needs providing insight to upper management for future and proposed systems ensuring they have the information needed to make those decisions to move forward Documents system information providing a steady state of information. Facilitates daily troubleshooting and maintenance of the day to day network infrastructure for over 500 end users as the subject matter expert (SME) ensuring continuity is in place for critical systems in the event of any possible failure Responsible for hands on coverage for over $2.8M in network infrastructure at both plant and mine locations assuring network and infrastructure systems are performing at peak efficiency and recommends improvements and or upgrades Installs and troubleshoots network systems which consists of the local area network (LAN), wide area network (WAN), wireless, VoIP and RFID readers so end users were provided a seamless network environment Responsible for the installation of over 400 Cisco VoIP desk set phones for the plant and mine location. This entailed disconnecting from copper land lines and replacing with TCP/IP network phones providing the network phone experience Installed and set up the CISCO wireless cell phones which enabled specific users to forward their desk numbers to a mobile wireless phone to carry within the entire corporate network offering them the opportunity to never miss a call Troubleshoots any VoIP phone issues at the desk prior to RMA of the device back to the phone provider resulting in more efficient tracking of true phone issues Maintains network local plant NOC where servers, plant security camera servers, call managers and phone networking equipment are housed along with the bundled T1's and Dmarc ensuring AC, electric and IP network cameras are able to monitor the environment in the event of disaster Standard System Architecture (SSA) team member in cyber security responsible for facilitating security policy, bringing plant SSA into NERC/CIP compliance in prep for audits, access control, physical security, end user security training, change control (CAB board) and IT governance for the plant control systems preventing possible plant control system compromise Presented corrective actions for local security systems when issues arise preventing unauthorized intrusion into local systems Performs system monitoring and bandwidth monitoring ensuring the network is in a healthy state along with maintaining tape backups and tape library Provides users with advanced network technical support, training and responds to needs and questions of users concerning their access of the network resource's for over 500 personnel while establishing, enforcing and disseminating IT security policy Monitors daily WAN traffic using Riverbed/Steelhead and Cascade optimization tools to ensure bottle necks do not occur reducing bandwidth and hindering worker production also providing daily reports of high use internet users Project-management effectively managing multiple projects concurrently at the plant and mine with direct involvement managing 3rd party vendors performing fiber/cat 6 and hardware installations Executes and ensures a direct communications path across all levels of management informing them of upcoming and changing requirements with system security and network operations keeping them abreast of changes in the IT space Peak performer as evidenced in midterm appraisals by management is responsible for oversight at 2 geographically separated locations for IT infrastructure security system related issues, network security, wireless networking, and network printing thus providing quality to all end users Environment: LAN/WAN, active directory environment (AD), desktops, laptops, switches, security, Cisco VOIP phones, Cisco Anyconnect VPN, end user training, installs and upgrades of servers, system patches, Xerox work center network printers and plotters, remote desktop/server access, RFID, wireless and mobile device email installs Education Certified Cloud Risk Management Professional CCRMP Bay State College July 2020 Certificate Austin Community College December 2019 Silicon Valley College Skills Business continuity, Cobit, Disaster recovery, Disk encryption, Dlp, Security Links http://www.linkedin.com/in/anelson2 Additional Information Technical Skills Platforms: Password management systems, Share Point, Microsoft Active Directory (AD), ADFS, VMware, Microsoft O365, wireless and hardwired environments. Applications: Microsoft Office (O365), (CASB) Cloud Access Security Broker, MS Project, Microsoft Share Point and Skype for business. Quest Kace servicedesk software, Password Management LastPass and Thycotic privileged account management (PAM), TrendMicro XGen server antivirus/behavioral learning, Digital Defense Frontline asset/vulnerability scanning, Solarwinds LMS, IPS, MetaCompliance security training courses, business continuity/disaster preparedness and various security applications. Access control, risk analysis, threat intelligence, Keypass and BitLocker disk encryption. AppRiver email spam and DLP management Other Skills: Establishes security policies, project management, systems management and overall leadership for IT related projects and initiatives. Managed and supervised employees in past positions. Maintains third party vendor oversight. Performs risk assessment, risk analysis and vulnerability scans to determine system vulnerabilities, access control, physical security weakness and standards for compliance and audit. Performed roles in COMSEC, OPSEC while in the USAF along with standards experience with Sarbanes Oxley, ISO, NIST, PCI, COBIT and HIPPA frameworks/standards. frameworks. Installs software packages, software patches and operating systems. Soft skills: Provides root cause analysis in the event of systems failures. Manages data loss/disaster recovery policy creation and standards along with risk management oversight. Possesses several years of leadership, management, projects, people skills, communication and an adept learner ready to take on new technology challenges. Proficient with educating and training end users on security risks in the enterprise and personal environments in addition with training and mentoring employees at all levels. . Strong work ethic, attention to detail, and drive to be successful. Extensive communications and written skills for all levels of management (C-Suite). Excellent problem-solving ability, including innovation, collaboration and analysis. Proficient in exercising judgment, discretion and decision making to resolve critical issues. Prior positions held include; Site Technology Coordinator/Manager, Network Manager, Helpdesk Coordinator/Manager and team lead. USAF Military veteran

Name: Mary Day

Email: joseanderson@example.com

Phone: 955.352.6761