Owner Owner Seeking Opportunity as a Security Analyst or Engineer Appleton, WI Hungry and seeking new opportunities Authorized to work in the US for any employer Work Experience Owner ACSP March 2018 to Present Partner Vendors: Check Point, Vmware, Cisco, Microsoft Azure, F5, Zerto SailPoint, Carbon Black. Leading Companies in their Sector Our Objective is to bring awareness to businesses regarding IT Security Standard and Tools. We strive to make technology integrate seamlessly with your business. Therefore, as your technology partner we will work hand and hand with you to support your growth. As our partner you will experience preferred customer service with direct Tier 2 support to our Partner Vendors. https://iabelsec.com/ IT Information Security Auditor Schneider November 2016 to March 2018 Conduct IT and IT-related audits. Perform risk analysis on systems and workflows used in business processes. Including analyses of business continuity/ disaster recovery, third-party relationships, contracts, and IT controls. Coordinate with colleagues compiling and organizing information in complete detail thoroughly and accurately for policies, standards and procedure documentation. Define and implement effective and efficient support models and processes. Manage and follow-up on open audit issues and ensure timely closure of action plans. Continually assess and improve the security of all systems utilizing automated technologies and manual processes. Risk assessments, Support Sarbanes-Oxley IT Compliance ISO- 27000 series, NIST, and COBIT methodologies and standards. Experience with OIM reporting, AD tools, PowerShell and Agile. Cyber Security Analyst Thrivent Financial November 2014 to November 2016 Managed the Vulnerability Management Service. Reported on identified vulnerabilities and assist in their remediation. Assist in identifying, managing and responding to potential security incidents. Detected vulnerabilities across corporate computing assets. Analyzed and reported any vulnerabilities to asset owners managed vulnerability remediation via ITSM Platform. Provided weekly vulnerability metrics to Information Security leadership. Reviewed, approved and maintained vulnerability exception requests Maintained relationships with IT domains contributing to the service. Monitored trending for both compliance and noncompliance. Creating and maintaining processes procedures and guidelines associated with the Vulnerability Management Service Performing technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). Supporting regulatory examinations and internal audits. Network Admin Guzman&Munoz Engineering&Surveying September 2012 to November 2014 Designed, analyzed, maintained and implemented LAN/WAN equipment and networks; work on all LAN/WAN installation projects. Develop technical policies and procedures regarding LAN/WAN activities. Provided technical support to all departments connected to the mainframe. Coordinated assigned service requests to meet requesting department dates within established department standards. Tested, evaluated and recommended selections of standard LAN/WAN components. Administered the LAN/WAN system. Designed, analyzed and implemented LAN/WAN equipment and design cost effective system configuration that meet the users' needs. Identified and resolved hardware and software problems. Made recommendations for new / altered technologies that would contribute to System cost savings and / or productivity improvements Coordinated capacity, planning and analyzed information concerning: Job-processing time, response time, hardware, software and voice utilization, CPU loads. Consistently monitor logs, dashboards and emails for conditions that may require manual intervention. Coordinated and control system tuning and hardware tuning and hardware integration. Ensure data / system security by protecting the corporate Information Technologies from unauthorized access, use or interruption. Coordinated the development of a comprehensive disaster recovery plan, maintain the plan, and conduct periodic testing. Inform Senior IT Manager of the status of system management issues. Network Specialist RgvCompuTech May 2010 to August 2012 Pm two locations for new Emrs. Backed up network data. Configured security settings or access permissions for groups or individuals. Analyzed and reported computer network security breaches or attempted breaches. Identified the causes of networking problems, using diagnostic testing software and equipment. Define and implement effective and efficient support models and processes. Documented network support activities. Troubleshoot network or connectivity problems for users or user groups. Provide telephone support related to networking or connectivity issues. Evaluate local area network (LAN) or wide area network (WAN) performance data to ensure sufficient availability or speed, to identify network problems, or for disaster recovery purposes. Analyzed network data to determine network usage, disk space availability, or server functions. Performed routine maintenance or standard repairs to networking components or equipment. Configure and define parameters for installation or testing of local area network (LAN), wide area network (WAN), hubs, routers, switches, controllers, multiplexers, or related networking equipment. Installed new hardware or software systems or components, ensuring integration with existing network systems. Tested computer software or hardware, using standard diagnostic testing equipment and procedures. Installed and repaired network cables, including fiber optic cables. Monitored industry websites or publications for information about patches, releases, viruses, or potential problem identification. Created and updated technical documentation for network installations or changes to existing installations. Trained users in procedures related to network applications software and related systems. Installed and configured wireless networking equipment. Maintained logs of network activity. Documented help desk requests and resolutions. Researched hardware and software products to meet technical networking and security needs. Created and revised user instructions, procedures, or manuals. Ran monthly network reports. Network Specialist FVTC August 2008 to May 2010 Tested computer software or hardware, using standard diagnostic testing equipment and procedures. Installed and repaired network cables, including fiber optic cables. Monitored industry websites or publications for information about patches, releases, viruses, or potential problem identification. Created and updated technical documentation for network installations or changes to existing installations. Trained users in procedures related to network applications software and related systems. Installed and configured wireless networking equipment. Maintained logs of network activity. Documented help desk requests and resolutions. Researched hardware and software products to meet technical networking and security needs. Created and revised user instructions, procedures, or manuals.

Experience Dell Managed Services Analyst SIEM Analyst - Arc Sight, Qradar, Splunk AV: Symantec Analyst IDP/IPS: Sourcefire Analyst, Snort Network Security NGFW: Check Point R77, Check Point Sand Blast Network Security Vulnerability tools: Qualys, Nesus AppSec: Imperva, F5

IAM: AD Tools, OEM, OIM, PowerShell 5.1 EDR: Carbon Black Vmware ESXI 6.5 - Currently Studying for VCP DCV Putty, Wireshark Netwitness Iron Port Security Controls - NIST 800-53, NIST CSF, ISO 27002 - Compliance - HIPAA Education BBA in Information Technology University Texas Rio Grande Valley Links https://iabelsec.com

Name: Jennifer Molina

Email: desiree93@example.com

Phone: 375.496.3285x536