Cyber Security Analyst - Senior Cyber Security Analyst - Senior Network Administrator/Systems Administrator Bossier City, LA Active DOD Secret Clearance expires in 2024. Strategic and forward-thinking IT Professional with a career history of effectively managing technical operations supporting organizational goals. Diligent and resourceful in uncovering solutions that meet all business needs; skilled at balancing resources and forging cross-disciplinary relationships to align business and technology objectives. Authorized to work in the US for any employer Work Experience Cyber Security Analyst - Senior General Dynamics Information Technology - Bossier City, LA April 2019 to June 2019 Role: Senior Cyber Security Analyst Works closely with Incident Management Team Supports annual incident response tabletop exercises Coordinates the development of reports from the SIEM, NIDS, and HIDS Supports annual updates of the incident response concept of operations document Assesses identifies and remediates issues of the individuals and/or systems affected Coordinates all information security incidents and comply with client-imposed deadlines Develops advanced analytics and countermeasures to protect critical assets Partners with IT leadership to support operational issues and prepares for potential incidents Leads major incident management efforts, supports agency leadership during major security incidents Develops, authors, and delivers process improvements for the Contractor Cyber Security Operations Center, to maintain operational readiness for incident response Monitors and reports on call volumes, alarm responses, and incident reports, ensuring contract s specified levels of service are met Works as part of a 24x7x365 team delivering real-time proactive monitoring and maintenance of supported security tools and associated rules and signatures Carries out triage on security events, coordinates incidents with Incident Management Team, IT Operations, Network Engineering, and Application teams, functionally supporting the Incident Management process Detects and analyzes incidents, coordinate activities with other stakeholders for containing, eradicating, and recovering from incidents IDS monitoring, network traffic and log analysis, prioritization, and differentiation between intrusion attempts and false alarms, insider threat and APT detection, and malware analysis/forensics Supports the production and maintenance of procedures, standard operational processes and playbooks Provides enterprise-wide management of security incidents and managed network space to detect, respond, and report all computer related incidents, to include daily monitoring of information systems, vulnerability remediation, intrusion detection, log review, and malware tracking Microsoft Exchange/Active Directory/Skype/Mobile Communications Engineer GDIT / CSRA - Bossier City, LA February 2017 to February 2019 TSA ITIP Government Contract Date: 2/11/2017 to 2/25/2019 Role: Microsoft Exchange/Active Directory/Skype & Mobile Communications Engineer Exchange, Active Directory & Mobile Communications functional areas; support the TSA network environment comprised of 80k+ mailboxes and 13k+ mobile devices Monitor and maintain Exchange servers, ensuring availability. Remediate Messaging Service Issues. We achieved our Email environment SLA 'uptime' goal, which was 99.8% for 2018 Ensure Active Directly Domain Controller availability across TSA sites/airports. Work closely with Tier 3 engineers to monitor and maintain the Email & AD environment, achieved SLA compliance goal of 99.75% Completed three significant migrations: Exchange Server upgrade from versions 2010 to 2016, Good Mobile Control to Blackberry UEM, FAMS AD/Exchange users/domain migrated to the TSA domain Create, maintain and remove Active Directory and mailbox accounts in an 80K user environment; use AD Toolkit and Windows PowerShell to generate reports. Grant rights to individuals and security groups. Create/update distribution groups, calendars, chat rooms, shared mailboxes. Support the Skype for Business environment, to include escalated end user incidents Apply Microsoft Security patches to Exchange/MCE servers using SCCM; places respective nodes in passive/standby mode by performing database activations and/or failovers Work with IAD Security Operations team to investigate security incidents and purge the enterprise mail environment during 'Spill' remediation Creates and maintains Standard Operating Procedures. Investigate and remediate end users' reported incidents, using the Remedy ticketing system. Thoroughly document incident timelines and actions performed. Perform AD/Email Bulk OIT Roster Screener Account Creation. This was a high-visibility and time sensitive process that had many defined steps; all steps had to be performed properly, and be done in a specific order. Process is performed in bulk using PowerShell scripting and AD Toolkit. Provide end user support for escalated incidents by phone, IM and email to the global TSA and FAMS workforce. Work with Tier 3 AD and Exchange senior engineers for incidents that require infrastructure modification. Monitor DB size, and migrate mailboxes to maintain free space and prevent downtime, to prevent the loss of business functionality, or mission critical systems or services IT Security Engineer Computer Sciences Corporation/CSRA - Bossier City, LA December 2014 to February 2017 Designs, tests, and implements secure operating systems, networks, security monitoring, tuning and management of IT security systems and applications, incident response, digital forensics, loss prevention, and eDiscovery actions. Conducts risk and vulnerability assessment at the network, system and application level. Conducts threat modeling exercises. Develops and implements security controls and formulates operational risk mitigations along with assisting in security awareness programs. Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access. Researches, evaluates and recommends new security tools, techniques, and technologies and introduces them to the enterprise in alignment with IT security strategy. Prepares security reports to regulatory agencies. Audits and manages access management. Design and conduct regular audits of computer systems to determine that they are operating securely, and confirm that data is protected from both internal and external attack Assesses assigned system to determine its security status and to ensure adherence to security policy, procedures and standards. Designs and recommends security policies and procedures Prepares training materials for computer security education and awareness programs; trains end users Monitors, evaluates, and maintains complex security systems according to industry best practices to safeguard internal information systems and databases Reviews security requirements and subsequently reviews systems to determine if they have been designed and established to comply with established standards Conducts investigations of security violations and breaches and recommends solutions; prepares reports on intrusions and provides analytical summary to management and client Reviews company firewalls logs across the organization and reports anomalies through chain of command Responds to queries and requests for computer security information and reports from both internal and external customers Provides recommendations concerning product upgrades, patches and other general security measures in order to enhance security controls across the diverse client architectures and systems IT Security Engineer PRISM, INC - Reston, VA April 2014 to December 2014 Engaged as a subcontractor and assigned to the TSA ITIP government contract by Prism, Inc. Six-month temp to perm hiring arrangement. Responsible for overall security operations of the TSA's network infrastructure. Analyze and execute security requests received from the TSA-SOC. Typically related to e-mail, network, application, and internet security. Performs risk assessments and completes documentation required for enterprise RFCs. Writes and updates SOPs to ensure the most efficient processes are in place. Network Administrator (50 Locatons/3 States) Ivan Smith Furniture - Shreveport, LA August 1996 to February 2014 Manage wide area network. Direct and develop key business requirements and IT strategies for technical projects. Manage IT operations and liaise between business and technical teams for organizational transition initiatives. Isolate and diagnose common Wintel system problems and document system events to ensure continuous functioning Coordinate and monitor troubleshooting, testing, upgrades, and configuration for all Wintel system files and services Analyze, log, track, and resolve complex issues pertaining to networking connectivity issues, printers, servers/applications Leverage business, technical, and interpersonal skills to manage center operations, customers, and operations personnel Managed 50 site networks - HP switches/Cisco Firewalls, Windows Servers, Active Directory, DNS, DHCP, Email, VPN Designed a strategy and deployed VOIP, which eliminated most POTS lines at the 50 locations, saving 17k per mon Added Unix and Linux servers to the enterprise to host Oracle databases and Oracle Forms for GERS and Red Prairie WMS Developed and rolled out an asset tagging program, tagging 4,865 IT devices at 50 sites located in three states in 36 days Designed and successfully executed Telcom/Data Center 'MOVE' project. Purpose was to transition all current operations from old site in Cedar Grove to a newly erected. Start-of-the-art facility. Was successful in the transition, and come Monday all data and personnel could operate in their new spaces. Departments involved were the corporate officers, HQ, Primary Warehouse Ops, Furniture Service Center, Mechanic's Vehicle Repair Center and Customer 'Pickup' Area all located within an integrated facility, in just a single weekend! My favorite piece was the state-of-the-art datacenter housed in an access-controlled, MASSIVE, seven-million-dollar HI-TECH complex, located on Technology Drive in Shreveport, La. This move compromised 150+ desktop users/computers, 14 servers, all software, databases, phones, data and the telecom services from six vendors. Plan included: surveillance systems, access control, data cable plant, a data center with redundant cooling systems, anti-static flooring and implemented a generator powered by natural gas, ensuring business continuity during very severe storms or post-hurricane Network Administrator HCA HIGHLAND HOSPITAL - Shreveport, LA February 1996 to August 1996 Novell Netware system manager GroupWise email system manager Manage physical access control system; administer users. Liaise with 3 rd party security personnel provider Evaluate, select and purchase all business server and desktop hardware. Diagnosis, troubleshoot and repair equipment Network Administrator HEARD, MCELROY & VESTAL CPAS, LLC - Shreveport, LA January 1992 to February 1996 Systems Administrator for Novell NetWare Novell Netware Network Supported all in-house hardware and software, to include ProSystem Tax Preparation Software; over 200 clerks, secretaries, partners and CPAs Worked 90 hours a week during the four-month long tax season each year Also supported our IT services clients, as an HMV IT consultant Evaluate, select and purchase all business server and desktop hardware. Diagnosis, troubleshooting and repair of physical office and IT equipment Education MCP certification in Microsoft System Administration Louisiana State University - Shreveport, LA September 2005 2 YR Vocational School Program Graduate in Network Systems Management Northwest Louisiana Technical College - Shreveport, LA January 1990 to December 1991 None in Data Processing and Accounting Arapahoe Community College - Littleton, CO Skills PowerShell (2 years), DNS (10+ years), DHCP (10+ years), Active Directory (10+ years), Group Policy, PKI, LDAP (10+ years), Identity Management, MS Exchange Email Administration (3 years), BES (2 years), Blackberry Enterprise Server (2 years), Good Mobile Control (2 years), Skype For Business (2 years), Firewalls (10+ years), McAfee Web Gateway (3 years), Antivirus (10+ years), Microsoft Outlook Support Expert (2 years), Email Administration (10+ years), Microsoft Office (10+ years), Technical Support (10+ years), IT Security (10+ years), Network Security (10+ years), Change Management (5 years), Routers (10+ years), Ethernet (10+ years), Windows Server Versions NT-2016 Server (10+ years), Microsoft Products - 27 years working with MS OS and Application Software (10+ years), Database Management (10+ years), Data Analysis (10+ years), ASA (6 years), PIX (10+ years), Switches (10+ years), Telecommunications (10+ years), Telephone Skills (10+ years), Analytical (10+ years), Detail-Oriented (10+ years), Software Deployment (10+ years), Software Evaluation, Implementation and Ongoing IT Support (10+ years), Excellent Written and Verbal Communication Skills (10+ years), Technical Knowledge Transfer - Clients and Teammates (10+ years), Troubleshooting (10+ years), Printers | Scanners | Copiers | Business Machines in Office Environments (10+ years), Document Management (10+ years), SOP - Creation, Review and Maintaining Operational Procedures Domumentation (10+ years), PBX (2 years), End User Support (10+ years), Windows 10 | 8 | 7 | Vista | XP | 98 | 95 | WFW and 3 and 2.0 Windows OS (10+ years), IT Purchasing (10+ years), Network Administration (10+ years), Networking (10+ years), NetWare (10+ years), Groupwise (10+ years), Novell (10+ years), IIS (4 years), File Management (10+ years), Backup and Recovery (10+ years), Tape Management - Rotation, Off-Site Storage, Tape Hardware and Software (10+ years), Business Continuity (10+ years), VPN (10+ years), Team Building (10+ years), Teamwork (10+ years), Knowledge Transfer (10+ years), POS (10+ years), WMS - IT System Management (10+ years), Wireless (10+ years), WiFi (10+ years), Mobile Device Management (10+ years), Billing Analysis - Telecommunications, Mobile and IT Bill Analysis, Tracking, Approval and Disputes (10+ years), Load Balancers (5 years), Cluster Management (5 years), Website Administration (10+ years), Product Management (10+ years), Maintenance of Technical Systems in Large Environments (10+ years), Security - Physical Premises Security Management (10+ years), Risk Assessment (10+ years), Field Engineering - IT and General Technical Systems (10+ years), Migration (10+ years), Project Planning (10+ years), Project Coordination (10+ years), Project Management (10+ years), Servers (10+ years), Hardware (10+ years), Proxy Servers (3 years), Symantec Endpoint Protection | SEP (5 years), Malware Prevention and Remediation (10+ years), Android | iOS | Apple | Windows Mobile Support, Administration, Management (10+ years), Unix Administration (10+ years), RHEL (3 years), Linux (3 years), DOS

(10+ years), Installation (10+ years), Technical Writing (3 years), Information Security (10+ years), Information Technology (10+ years), Information Assurance (10+ years), Surveillance Systems | Site Evaluation, Implementation and Management (10+ years), Video Surveillance Systems Management (10+ years), Identity Management (10+ years), Account Management (10+ years), Barracuda (1 year), Mirapoint Email System Management (1 year), SCCM (Less than 1 year), WSUS (1 year), ePO (1 year), ePolicy Orchestrator (1 year), Bitlocker (1 year), Symantec Endpoint Encryption | SEE (1 year), Forefront | Microsoft Forefront (5 years), Encryption (3 years), Outlook Support - Tier 2 and Tier 3 (2 years), SiteProtector (3 years), IDS (3 years), HIDs (3 years), NIDs (3 years), Websense (1 year), McAfee Email Gateway | MEG (1 year), ArcSight (3 years), Intranet (2 years), Sharepoint Administration (Less than 1 year), Winmagic (1 year), Disaster Recovery (10+ years), Endpoint Management (10+ years), RDP (10+ years), PAM (2 years), Priviledged Access Management (5 years), Xceedium (5 years), Remedy | BMC Remedy (5 years), Ticketing Systems Administration (5 years), Customer Service Skills | Exceptional Customer Skills - References Available! (10+ years), Customer Relations | CRM (10+ years), Vendor Management (10+ years), Vendor Relationships (10+ years), Customer Service (10+ years), CRM (2 years), Customer Relations (10+ years), Customer Relationship Management (10+ years), Service (10+ years), Certified Software Manager (10+ years), People Person (10+ years), Executive Support (10+ years), Excel (10+ years), Spreadsheets (10+ years), Wordperfect (5 years), Word (10+ years), VI | Virtual Editor (10+ years), Virtualization (3 years), Bomgar (2 years), SPAM (10+ years), Email Filtering (10+ years), Accounting Systems Installation and Support | Administration of Tax and Accounting Software (3 years), Desktop Support (10+ years), Laptop Support | Notebook Support | iPad Support | Tablet Support | Portable Device Management (10+ years), Access Controls Systems (10+ years), Interviewing (10+ years), Assessment (10+ years), Inspection (10+ years), Cross-Functional Team Leadership (10+ years), Microsoft Exchange, System Administrator, System Admin, Red Hat, Linux Administrator, Exchange Server (2 years), Redhat, ServiceNow (Less than 1 year) Certifications/Licenses CompTIA A+ Present CompTIA Network+ Present Certified NetWare Administrator Certified Software Manager Microsoft Certified Professional (MCP)

Name: Tara Wells

Email: rodrigueznicole@example.net

Phone: +1-628-610-2016x533