

Information Security Analyst Information Security Analyst Information Security Analyst - XTO Energy
Houston, TX Work Experience Information Security Analyst XTO Energy January 2018 to Present
Create monitoring alerts and review the performance of log analysis using the Splunk SIEM tool while actively monitoring for any anomalies then remediating if so. Responsible for the creation and management of application & user access reviews while maintaining regulatory compliance. Creation and management of all membership groups through Active Directory to ensure all groups are within compliance. Contributed to establishing the XTO Identity lifecycle policy for all employees for provisioning, de-provisioning, recertification, and auditing. Developed and reviewed company policies for change management, incident management, and threat remediation while collaborating with senior company leaders to ensure best practice was being ensured. Analyzed and responded to all identity management technical and process failures. Collaborated with fellow security team members and management to review and evaluate risk assessments. Also made notice of any software or hardware changes needing to be made and then implemented those changes. Administered and maintained privileged access security utilizing CyberArk Enterprise Password Vault.

IT Security & Desktop Support Analyst HMT Tank Incorporated December 2016 to January 2018
Image Deployment & profile setup of Windows 7, 8, and 10 devices such as Desktops, Laptops, and Tablets using Dell Kace 2000. Verify that all system drivers are up to date, and all needed applications are installed. Mobile Device Management, and phone activation for enterprise users utilizing the Mass360 application. Setup & management of multi-function print/scan devices such as HP, Ricoh, & Xerox. Responsible for repair and maintenance as well. User account and Device management within the company Active Directory. Management of account permissions, access, and group policies. Email account creation and management within our company's Exchange server. Manage, Secure, and Backup storage and data files within our company servers utilizing Windows Server 2012 and Windows Server 2016. Monitor and respond to incoming threats using the Webroot application. Mitigate and quarantine threats using applications such Malware bytes, Super-anti Spyware, and Ccleaner. Daily support of Microsoft Office 2007, 2010, and 2013 applications such as: Word, Excel, Outlook, Skype for Business,

Access, etc. Patch management, Software distribution, IT asset and Inventory management using Dell Kace. Event log review to determine root cause analysis of security and system events. Load balancing utilizing Cisco Catalyst switches & Palo Alto networks. IT Desktop Support Analyst University of Texas MD Anderson Cancer Center December 2015 to October 2016 Provides technical support to end users to resolve basic, moderate and complex computer software and hardware issues in Windows 7, 8, & 10 environments. Utilized SCCM 2012 to create & deploy software packages, Deploy patch updates, and to schedule & run tasks on devices in the directory. Assigns access permissions for members & groups through Active Directory using Group Policy. In accordance with HIPAA, Identified organizational risks and escalate appropriately. Account administration through Active Directory. Unlocking user accounts on the domain and managing user account passwords for network authentication. Provides support for hospital wide applications such as Citrix, Epic EHR, VMware, etc. Analyze and respond to security incidents. Monitor intrusion detection & prevention. Review, and audit system & event logs, Verify data loss protection. Provides technical expertise for troubleshooting connection issues in a LAN & WLAN environment. Performs image building & deployment on organization assets using ICD/MDT. Able to manage, monitor and support IT Security technologies, including but not limited to Email SPAM filtering solutions, vulnerability scanning solutions, Intrusion Detection Systems, anti-virus software, & Internet web filtering solutions. Tier 2 IT Support Analyst Amedisys Home Health & Hospice June 2014 to September 2015 Performed software installation via Remote Desktop and supported those applications via user call in, email, and chat requests in Windows 7 & 8 environments. Performed image building & deployment on organization assets using ICD/MDT. Performed new device setups and configurations for clients & management. Ensured the quality of the installations and applications to the highest standard. Also completed the installation of printers & scanners. VPN provisioning. Answered and resolved user ticket submissions through CA Service Desk Manager. Averaged 20 tickets per day. User accounts management through Active Directory. Unlocking user accounts on the domain and managing user account passwords for network authentication. Performed system, and account auditing using syslog. McAfee drive encryption updates for end

users to ensure asset protection. Ran routine system security scans & updates to ensure there was no malicious software within the host or files using VirusScan Enterprise, I would quarantine and remove threats if so. Performed deployments, Patch updates, & Policy enforcement to host devices on our company network using ePolicy Orchestrator. Analyze & respond to security events. Responsible for troubleshooting connection issues in a LAN & WLAN environment. Installation of wireless air cards for client laptops. Performed Cisco Firewall administration, and troubleshooting. Managed program folders and confidential data files on our company servers. Android & IOS mobile phone support, Installation and app support, also remotely managed mobile devices to ensure company policies were enforced. IT Support Analyst Cox Communications May 2012 to June 2014 Utilized Landesk Service Desk to support users and client base by resolving problem tickets.

Performed network troubleshooting & diagnostic repair. Monitored network security alerts using the Norton security suite manager. Utilized Landesk to manage the company's assets & inventory. Also performed patch management, monitoring, scanning & repairs. Performed application packaging & deployment using Landesk as well. Education AAS in Cyber Security Baton Rouge Community College 2017 to 2018 MCSE Houston Community College Skills Active directory (4 years), intrusion (Less than 1 year), Metasploit (Less than 1 year), network security (2 years), Scripting (Less than 1 year), Security (6 years), Snort (Less than 1 year), Splunk (1 year), Switching (Less than 1 year), Websense (Less than 1 year), Windows server 2008 (Less than 1 year), Wireshark (Less than 1 year)

Name: Brian Baxter

Email: mendozacarlos@example.net

Phone: 929-935-1487