

Information Security Analyst Information Security Analyst Information Security Analyst Richardson, TX Skilled and self-motivated information security professional with 4 years of experience in Access Controls, Security Operations & Administration, Risk Identification, Monitoring & Analysis, Systems & Application Security, and Vulnerability Management of a wide range of systems. Well-versed in direct and remote analysis with strong critical thinking communication and people skills. Work Experience Information Security Analyst Texas Capital Bank - Richardson, TX November 2018 to Present IT Security Analyst TEXANS CREDIT UNION - Richardson, TX November 2015 to November 2018 Contributed to the security team by being involved in the fine tuning of the intrusion detection system (IDS/IPS) as well as having to respond to incident alerts generated by the SecureWorks SOC. Managed the Firewall content filtering alerts generated by Network Engineers when performing a change to the Firewall, and analyzed differences to the approve changes. Able to lead, develop, coordinate, and execute actions within the Cybersecurity Incident Response plan, and threat management plans. Key Contributions: Manage the inflow of vulnerabilities from various systems. Coordinated with Systems and Network engineers regarding the re-mediation of vulnerabilities on Cisco Switches and Routers, and applications on different Windows 2008/2012 servers. Conducted research for vulnerabilities to provide to engineers and verified vulnerabilities were fixed based on vendor recommendation or best practices. Due diligence through constant monitoring. Monitor real-time security alerts and identified and prioritized potential threats, from our SolarWinds SIEM and correlate that into different security systems to understand a threat behavior and activity. Created reports for management to take actions on different findings regarding potential threats to the enterprise. Risk management. The NIST Framework was used as a guide to conduct analysis about a potential risk and identified, assessed, and responded to risk tolerance activities and informed business key owners about the risk level for a system or activity in the organization. Coordinated with the system or process owners' to mitigate, transfer, avoid, or accept the risk depending on the potential impact to the organization. Keeping up with latest security trends. Became a member of the Financial Services Information Sharing and Analysis Center to gather threat intelligence. Analyzed alerts and conducted verification for any vulnerable systems in the

enterprise, and if so then created a plan of action to respond to the threat. IT Helpdesk Analyst
CARDIOVASCULAR PROVIDER RESOURCES/HEARTPLACE - Dallas, TX 2014 to 2015
Troubleshooted technical issues reported by Cardiologist and corporate staff in a fast pace
environment constructed of 27 clinics across the DFW area. Trained Cardiologist and Healthcare
staff on new technical solutions acquired by the company such as Office 365, and new Windows 8
operating system. Able to decrease active service tickets on average from 100 a week to less than
20. Key Contributions: Orchestrated knowledge base repository for helpdesk. Served as lead
on a new ticketing system for helpdesk in which knowledge base articles were written and stored to
help the team reference resources from previous similar issues for a more efficient workflow.
Trained Cardiologist on new dictation software. A total of 50 Cardiologist were successfully
instructed on how to use the new dictation software (Dragon), and served as the primary contact for
any issues. Facilitated upper management with reporting. Created weekly and monthly reports on
(desk.com) to show progress on closed tickets or status reports on outgoing projects, on average
generated 20 reports a month. IT Intern BLUE CROSS BLUE SHIELD OF MICHIGAN - Detroit, MI
2014 to 2014 Supported employees with technical issues associated to their laptops and software
such as Outlook or WebEx. Explained employees best practices for the usage and maintenance of
their laptops and coordinated the deployment of any new laptops to employees. Key
Contributions: Created weekly blogs related to technological topics. In SharePoint a weekly blog
was created discussing new trends on IT or new devices coming into the market, also tips were
written regarding basic troubleshooting to laptops that employees could use. Advice employees
on any questions regarding new laptops. New laptops were given to employees, support on any
functions or basic maintenance practices were explained to employee. Education Bachelor of
Science in Technology Management TEXAS A&M UNIVERSITY - College Station, TX 2015 Skills
CISCO (3 years), FIREWALL (3 years), IDS (3 years), INTRUSION (3 years), INTRUSION
DETECTION (3 years), Access Controls (3 years), Threat Intelligence (3 years), Incident Response
(3 years), Data Loss Prevention, Systems & Application Security (3 years), Risk Management (3
years), Active Directory, Security, access Links <http://www.linkedin.com/in/jscastaneda>

Certifications/Licenses SSCP Additional Information Technical Skills SecureWorks, IDS/IPS, Zscaler Web Filtering, Windows 7/10, Server 2008/2012, Intrusion Detection, Cisco Firewall Review, Cisco Meraki Wi-Fi, Endpoint Security, Web Development, HTML5, MS Office Suite, MySQL, Active Directory, Switch Management, Citrix Receiver, WSUS, SolarWinds SIEM, Change Control Management, packet capture

Name: Blake Lee

Email: jasonmorrison@example.net

Phone: +1-377-579-3487