

Senior Security Engineer Senior Security Engineer Senior Security Engineer - SeneGence International Orange, CA Work Experience Senior Security Engineer SeneGence International April 2019 to Present Security Governance - Governance statement and Framework created for senior management. Security Controls NIST 800-53 - Program created to assist corporate certification. Risk Management NIST 800-37 - Framework program created to assist in corporate risk management. Asset Management - Discovery to determine the scope of the environment. Policies - Implemented BYOD and Acceptable Use policy. Auditing - Gap analysis to determine current PCI/DSS standards to the current environment. Reports created for Senior Management. Nessus Vulnerability Scans - Scans completed for internal, external and cloud environments to Identify risk and providing mitigation solutions to Senior Management. Change Management - Framework for ITIL was created and presented to senior management. Budget - Security program budget presented to senior management. Security Awareness Training Monthly user campaigns and training using KnownBe4. Infrastructure Operation Supervisor ATOS April 2017 to March 2019 Management - Managed a team of 15 network engineers. This included career development and managing the on call scheduling. Support - Supported over 3000 network and security devices for the County of Orange Identity and Access Management - Managed access control on all devices through TACACS+, Infoblox, NetMRI, wireless controllers and shared drive. Project Management - Managed multiple network and security projects that included configuration management, standardize security protocols, code standardization, standardized network protocols and architectural design corrections. Red Seal Vulnerability Scans - Mitigate identified vulnerabilities on security and network devices. Analysis - Network optimization and ongoing scans to determine potential security risk. Reporting - Coordinated a wide array of daily, weekly and monthly reporting for internal operations and sensitive Information. Troubleshooting - Primary management to triage all task and Incidents. On Call - Primary Management Escalation for daily and weekend on call. Compliancy - SOX, HIPAA and PCI/DSS Network Security Engineer ATOS August 2015 to April 2017 Part of firewall team that maintain a network security within the County of Orange County. Firewalls - Configure ACL's, NATs and VPN's. Troubleshoot - Connectivity issues throughout the

enterprise and provide access issues through the firewalls, Nexus routers and switches and Layer 2 and 3. Testing - Responsible for complex testing and analysis of all network. Network Security - Troubleshoot and resolve areas of identified risk. Scans - Packet capture and analysis with PCAP Visio Diagram - Creation and management of all LAN and WAN design. Wireless Network - Managed and provided troubleshooting for Cisco and Enterasys devices. Senior Security Specialist St. Joseph Health - Palo Alto, CA December 2013 to July 2015 Cisco Stateful Firewalls - Configuration and management of ACL's and NAT's ASA - VPN Configuration and Management. Palo Alto ? Firewalls - Deployment, configuration and management of firewall policies. ? Traps - Deployment, configuration and management on end point devices. ? Panorama - Configured, deployed and managed devices across the environment. ? IPS/IDS - Configuration and management of policies to mitigate threats and vulnerabilities. McAfee ? ePO Antivirus. ? Data Loss Prevention - ? Web Gateway - Implementation, Changes and Repairs. ? Enterprise Vulnerability Scans ? Web Reporter - Implementation and design of various reports for Management and HR review. Checkpoint Firewalls - ACL and policy configuration and management. Sonicwall Firewalls - ACL and policy configuration and management. SSL Certificates - Implementation, revocation and renewals. Identity and Access Management - Managing and deploying secure key management on Dell TPAM. Architecture Security Design for Northern and Southern California. Citrix Netscaler Management Expert Change Management Skills. Compliancy - HIPAA and PHI. IT Security / WAN Administrator Kaiser Aluminum Corporation May 2013 to November 2013 Change Management - Implemented and managed based on ITIL Project Management - Managed multiple security implementations across the LAN and WAN. Firewalls - Managed and configured Cisco ASA 5510 and 5505 Firewall ACL and policies. Web Proxy - Configured and managed SOPHOS Endpoint and Web Proxy through white and black listings.. Proofpoint - Managed the Spam Filter. Testing - Checkpoint and Palo Alto Firewalls to determine vendor of choice. Networking - Implement and manage Cisco 2950, 2960, and 3750 switches. Cisco 3560, 3570 Switch Stack and Cisco wireless network. Troubleshooting - Meshed MPLS network. Testing - Aruba, and Cisco/Meraki wireless devices determine vendor of

choice. Daily management of the SysLogs. Security Controls NIST 800-53 - Program created to assist corporate compliancy. Auditing - Performed site surveys for Security and Wireless needs. Compliance - Knowledgeable in SOX and SEC requirements Network Engineer Orange County Sheriff Department November 2012 to April 2013 Network Devices - Installed and implemented Cisco Routers, Switches Installed and implemented Cisco Access Points. Monitoring - Monitored the network through SolarWinds. Firewalls - Monitor Cisco ASA's. Project Management - Managed several major network projects within the jail system. System Administrator Delcan Corporation April 2012 to June 2012 Networking - Configuration management on Cisco routers and switches. Firewalls - Manage and configure ACL's and policies on Juniper, Barracuda and Cisco PIX Firewall Troubleshooting - NetFlow network sniffer using Wireshark. Endpoint Protection - Symantec Endpoint Protection Virtual Servers - Implemented and managed Hyper-V on 2008r2 servers Network Administrator Premier Business Center November 2011 to March 2012 Troubleshooting -VPN access, router and switch configurations. Networking - Configure and Manage Cisco and Juniper routers, switches, PIX and servers. Monitoring - NetFlow Analyzer and Wan Spy. Firewalls VPN's management through SonicWall and Cisco. Configurations - NAT and global commands on Cisco Routers and PIX. Servers - Configuring Dell Servers with VNC, NetFlow and Antivirus software. Active Directory - Configuring IPP in active directory and managed Active Directory on a corporate level. Education Diploma in Information Technology in Information Technology Stanbridge College - Irvine, CA 2011 Bachelor of Science degree in Health Science California State University 1999 Skills CISCO, ENCRYPTION, FIREWALLS, ITIL, PCI, Information Security, Siem, Network Security, Cissp, Palo Alto Additional Information Specialties: Leadership, Compliance, Auditing, Project Management, Security Consulting, CMDB Management, Reviews, Technical Project Manager, WAN and LAN design and deployment Cisco devices (Nexus), Juniper Devices, Microsoft infrastructure, Public Key Infrastructure, F5, Infoblox, AV Architecture and Deployment, HIPPA, PCI, ITIL, COBIT, SOX compliance, encryption architecture. Experience with, ASA and Palo Alto Firewalls, Palo Alto IDS/IPS, McAfee DLP, McAfee Proxy, McAfee Vulnerability Scans, Extreme Wi-Fi, Cisco Switches/Routers, Alcatel Switches, Brocade Switches,

HP Switches, Dell Switches. Very competent with Layer 2 and Layer 3 troubleshooting. Packet capture and analysis. Experience with ITIL and Change Management. County and Federal clearances. Relocation: Yes

Name: Michael Brown

Email: alex84@example.org

Phone: 001-569-816-7172x865