

Security Administrator Security Administrator Security Administrator - Pacific Premier Bank Fullerton, CA An ambitious Cyber Security Engineer with excellent interpersonal and critical troubleshooting skills. Proven asset within a growth-oriented organizations. Unique ability to quickly adapt and learn new and emerging technologies while applying innovative solutions to existing organizations architectures. Work Experience Security Administrator Pacific Premier Bank - Irvine, CA February 2018 to Present Currently working with Pacific Premier Bank Security Group serving as the Cyber Security Pillar and Lead Engineer for Web Gateway, Email Gateway and network threat monitor. Additional duties include providing architectural, engineering and operational support for enterprise Cisco Identity Service Engine (ISE) and Cisco NGFW. Responding to security incidents as part of the incident response team. Participated in disaster recovery test in moving and monitoring critical system from primary data center to the alternative data center. Manage and optimized Cylance protect and optics

- o Mitigated malware from executing on the endpoint with Cylance protect
- o Stopped private data from leaving the hard drive with Data Loss Prevention
- o Optimized Cylance exclusions to work with vendor applications
- o Updated Cylance products to the latest version after they were tested
- o Monitored and created dashboard to make sure system where up to GBLA/FRB compliance

Manage and optimized ProofPoint Email Gateway (MSC) System

- o Implemented dynamic blacklisting through MSC signature inspection and 3rd party blacklist.
- o Optimize ProofPoint performance through system updates, architectural revisions, and policy enforcement
- o Block SPAM from propagating across PPBI.com by leveraging alerts to identify propagating SPAM and phishing campaigns
- o Monitor and blocked Malware Activity propagating through the email attack vector by fine tuning SPAM and Packet inspection policies
- o Ensure the confidentiality, integrity and availability of Pacific Premier Banks Email Architecture
- o Stopped unauthorized spoofing activity by creating a block rule that inspects header from traffic for display name mismatches

Manage and optimized ForcePoint Web Gateway (Proxy)

- o Ensure the confidentiality, integrity and availability of Pacific Premier Bank Web Architecture through policy
- o Minimize user web activity risk by blocking malicious websites and content
- o Detect and block malware before it is delivered to an endpoint
- o Enforce Pacific Premier Bank values and policies

through web content filtering o Ensure the confidentiality, integrity and availability of Pacific Premier Banks web access o Optimize Web Gateway performance through system updates, architectural revisions, and policy enforcement o Created individual user web access groups accounts for different business departments

Security Engineer, Consultant St Joseph Health - Anaheim, CA June 2016 to January 2018 While working with St. Joseph's Health Ministry Security Group serving as the Security Network Pillar and Lead Engineer for McAfee's Security Information and Event Management (SIEM) system, McAfee's Email Gateway (MEG) and McAfee's Web Gateway (Proxy). Additional duties include providing architectural, engineering and operational support for enterprise Intrusion Prevention System (IPS) and Firewall systems from Palo Alto Firewalls, Cisco ASA and preventing exfiltration of data with McAfee DLP.

Information Systems Technologist Consolidated Networks - Fort Irwin, CA February 2015 to May 2016 Monitored systems with ePolicy Orchestrator. To make sure that the systems & servers have the latest antivirus software installed so they can be on the network. At the same time make sure that users are not plugging in personal USB, CD drives or smart phones devices to the systems wanting to retrieve classified information from these systems using data loss prevention. Perform Security Content Automation Protocol scans to make sure that the systems are all in the same baseline. Weekly vulnerability scans on systems using Nessus vulnerability scanner to make sure that patches are up to date on systems & servers. Monitored network and system events with Splunk (SIEM). Helped my team with Risk Management Framework audit so that the company could keep their accreditation. Regular weekly backups of servers and network logs to be prepared in case of incident that may occur. So that any member could bring back up the systems as quickly & efficiently as possible.

Electrical Rebuilder, Equipment Truck Electric - Hesperia, CA March 2010 to January 2015 Troubleshoot, fault, isolate, rebuild and repair alternators, starters and electrical motors for heavy machinery, big rigs, HMMWV and general vehicles. Troubleshoot stators, armatures, diodes, rectifiers and all other inter components within a starter and alternators. At the time I would administrate and configure the office equipment. I would update the computers with the latest windows patches. Configure the firewall/router to allow for wireless printing for credit card

receipts. Ran cat5 cabling to have wireless access points around the building. 2538 Associated
Rd, Fullerton CA 92835 760-338-5452 castellanose88@gmail.com Skills Ccna, Information security,
Nessus, Qualys, Siem Additional Information Skills and Qualifications Certifications and Technical
Skills Compliance and Mitigation Cisco CCNA Software Risk Assessment Security plus SYO
401 Hardware Risk Assessment Palo Alto Networks ACE SOP documentation McAfee
ePolicy Orchestrator (HBSS / ePO) Nessus Vulnerability and Risk Analysis McAfee Virus Scan
Enterprise Risk Management Framework Compliance Audit Cylance Protect Server Hardening
for Compliance Dell Secure Works Monitor and Alerts WorkStation Hardening for Compliance
McAfee Virus Scan Command Line Scanner for UNIX/Linux System security scanning McAfee
Web Gateway (MWG) IT controls - design, operation and testing McAfee Email Gateway (MEG)
Information Security Monitoring Conducted Annual Risk Assessment McAfee Enterprise
Security Manager McAfee Security Information Event Management(SIEM) System vulnerability
Assessment Splunk SIEM Cisco Identity Security Engine (ISE) ForcePoint Enterprise Security
Manager ProofPoint Email Gateway Cisco FMC and FTD Palo Alto Firewall Administration
Palo Alto Traps Administration Vulnerability Scanning and Reporting
Nessus/OpenVAS/Qualys Intermediate user of Kali Linux Windows server/workstation
administrator DarkTrace Threat Monitor

Name: Matthew Burns

Email: michaelflores@example.com

Phone: 611.404.7411