IT Security/Administrator/Consultant- Security Operations IT Security/Administrator/Consultant-Security Operations IT Security/Administrator/Engineer- Security Operations - Response and Solutions Oakland, CA To use my advanced knowledge of the computer industry, including media, network & system solutions, security, and business applications, to obtain a secure position in computer security operations and infrastructure with opportunities for advancement Authorized to work in the US for any employer Work Experience IT Security/Administrator/Consultant- Security Operations Response and Solutions April 2019 to Present first point of contact for escalations, Executive Leadership Team support; Management of servers and technology tools, Monitor performance and maintain systems according to requirements and lead of incident investigations (CrowdStrike, SEP, 0365, Azure, Palo Alto Firewalls); ensure security through access controls, maintain IT & InfoSec Procedures and Documentation; team Lead for Helpdesk & Security departments; helped scale down ticket SLA's 40% with automation processes and quicker response times; manager of all security infrastructure, procedures and incidents Sr. Researchist & Consultant, IT Support & Security, Bay Area techNotics October 1994 to Present specializing in Operations, Administration & Security in corporate/production/cloud/24-7 live environments, backend solutions, real-time monitoring, efficiency, scaling and metrics in Linux/Unix environments and Windows environments, security specialties in vulnerability scanning, security assessments, penetration testing, web app security, OWASP and WASC proponent and advocate; and security consulting using Windows, NIX, OSX, open-source and commercial tools, familiar with Approved Scanning Vendors and PCI Compliance procedures; PCI-DSS requirements Staff Security Engineer Blackhawk Network Holdings February 2018 to February 2019 Tier 1-3 Incident responder, staff on Cyber Defense Center monitoring, handle all incidents using: Splunk, CrowdStrike, DarkTrace, Anomali, Symantec Endpoint, Microsoft Advanced Threat Detection, Signal Science, LogRhythm; Security engineering projects for deployment of Symantec DLP and Imperva SecureSphere for enterprise database environment for gift card network; monitoring of all Blackhawk internal services and assets and acquisitions; almost 30 acquires up to 2018; Tenable Nessus vulnerability scanner SOC Engineer II/Penetration Tester - Audit, Regulatory & Compliance

firm Adhere, Inc September 2017 to December 2017 SOC Level II duties and monitoring for external clients, SIEM-AlienVault main monitoring channel, incident response engineer for external clients; penetration tester for managed clients including: methodology, security assessment and impact based penetration testing on systems, networks and applications; engineer for threat analysis and vulnerabilty research, threat research & intelligence for tools and process implementation techNotics April 2016 to August 2017 Private clients for owned company, techNotics, including: incident repsonse, security assessments, penetration testing, post-incident assessments, consulting on security solutions; Clients can be disclosed per case basis, depending on NDA agreement with each prospective client: main tool concentrations on Tenable Nessus, Nexpose, OpenVAS, and Qualys for first level scanning weekly of assests, scheduling and common vulnerability awareness; Linux/UNIX hardening, security standard implementation advisement for servers & production nodes; DNS security monitoring and consulting, big risks in the last few years have been: Typosquatting, DDos, Amplification attacks, resolver attacks, cache poisining, registrar hijacking, more intricate vulnerabilities such as phantom domains, nxdomain, random subdomain (slowdrip); some services used for security have been DNSSEC, DNS Crypt, implementation of scrubbing services like Prolexic (now Akamai), and proxies such as CloudFlare The Gap - Palo Alto, CA October 2015 to April 2016 The Gap (October 2015-April 2016) - Security engineering of enterprise solutions, that encompass-DLP, key mgmt. and rotation, vulnerability scanning, SIEM, remote access lockdown, security testing of applications and tools deployment for incident response, including Bit9+CarbonBlack, Splunk, Palo Alto, Akamai/Prolexic, Tenable Nessus and Cylance; SOC inception Datapipe/GoGrid March 2015 to September 2015 Security assessment, incident response, engineering, consulting, solutions & security management; SSAE 16 SOC 1 compliance assurance Security analyst Riverbed Technology September 2014 to January 2015 tester active in security operations, incident response & monitoring using Splunk, Riverbed Cascade, Vectra, Palo Alto Firewalls, SourceFire IDS, Tenable Nessus, FireEye and Burp Suite; enterprise architecture, design and deployment; SOC creation Information Security Analyst active in security operations Riverbed Technology September 2014 to January 2015 incident response & monitoring using

Splunk, Riverbed Cascade, Vectra, Palo Alto Firewalls, Sourcefire IDS, Tenable Nessus, FireEye and Burp Suite; enterprise architecture, design and deployment; creation of SOC and Incident Response program; and internal pen testing process VMware March 2014 to August 2014 using NetWitness, zScaler and Splunk for malware/DDos/forensics/botnet detection for their SOC Sr. Security Engineer The Gap March 2012 to January 2013 contract through Advantis Global-responsible for implementation of security solutions, mainly Palo Alto Networks firewalls, Lockpath-Keylight GRC, QRadar Q1 SIEM, administration of Qualysguard Enterprise; implementation of Rapid7's Tenable Nexpose/Metasploit Suite for the enterprise, Tripwire/OSSEC for Infrastructure servers, and Bluecoat for Enterprise proxy; Tenable Nessus vulnerability scanner recently implemented; constant security audit's weekly with scanning & manual testing; SOC creation and training; internal pen testing Seasonal The Gap 2012 to 2013 2012-2013) - Web app pen testing for gap.com; established a web app/network security program that concentrated on-protocol support, authentication, authorization, session mgmt., crawling, parsing, client-side attacks, command execution, Information Disclosure, exploits & remediation Bay Benefits -http://www.nfp.com/nfpca/ - Seasonal penetration testing including network security, web app security, domain presence, public footprint and DDos potential Seachange -http://seachange.org/ - Seasonal pen testing mostly whitebox in network and web, emphasis for organization on reputation, and exposure from the public Official Role Titles & Description: Security Systems Engineer Sephora, Inc September 2011 to December 2011 contract through Insight Global-responsible for creation of automation scripts for secure transfer project involving Sephora's vendors, securing process and evaluating flow, accuracy and efficiency, interaction with vendors to help establish and finalize security transfers, via sftp, ssh, and public encryption keys (gpg & pgp); Support Engineer, Support Groundwork OpenSource July 2011 to August 2011 for network monitoring software-Groundwork in the open source community. Multi-Tier for customer usage issues, escalations, work closely with QA and Engineering. Strong UNIX/Linux sys admin support, along with Apache, MySQL, and PHP LAMP stacks; configuration issues and management; strong use of JIRA; security advocate-http://gwos.com Technical Support Engineer Xobni, Inc June 2010 to

February 2011 Tier 1-3 support for Xobni software (Outlook plugin, Blackberry client, cloud service) products; QA, bug tracking, testing, Zendesk, JIRA, and Metova used for ticketing system and collaboration; security advocate http://www.xobni.com Operations Engineer Pivotal Labs, Inc September 2010 to December 2010 Support & System of 90 team Ruby Developer environment, system, network (HP hardware), and support operations, automation scripts (shell, python), code integrity and versioning (svn, git) in an OSX & Linux environment, Ubuntu Enterprise Cloud management-Eucalyptus powered; security advocate-http://pivotallabs.com Mail Security Engineering Analyst, Anti-Spam Yahoo April 2010 to June 2010 analyzing, honeypot network creation, projecthoneypot.org collaboration, account seeding, tracking and logging; succeeded on making their webmail spam filter more efficient by 40% Systems Specialist, System Administration, Network Administration and workstation support NeuroFocus, Inc December 2009 to April 2010 for neuroscience marketing company; Corporate IT in a NIX backend environment, colocation administration, web application maintenance and security; OSX Client environment, and Windows business applications; security advocate-http://www.neurofocus.com IT Administrator Prospect Sierra Middle School February 2009 to December 2009 user support and system Administration and trainer for users in OSX server and OSX client environment, Altigen PBX administrator, OSX servers running dns, afp, webobjects, dhcp, proxy server, mail server (Postini), secure login, php, mysql, perl/python services, vpn server, ichat server; security advocate http://prospectsierra.org Sources, Senior Analyst Publicis-re - San Francisco, CA October 2007 to October 2008 -Assistant Operations Manager-Senior Support engineer, OSX, Linux & Windows platforms, supported well respected advertising Agency with 9 different business units, designer support in graphics, video, media. Network, Administration and Security support of file servers, mail servers (Exchange 2003-07), data backup servers, web servers (Apache), running Windows 2003 server, OSX 10.4 & 10.5 Server, and multiple flavors of Linux, support of smart phones, administration of Cisco Wireless LAN Solution, Lotus Notes, VPN, Fiery print servers, Novell eDirectory Administration, VMWare Manager, Oracle VirtualBox, Ubuntu KVM, Ubuntu Enterprise Cloud IT Specialist, Oakland Office of the President October 2004 to October 2007 Support and help desk for 139 users in the office of the President on

a Windows XP/OSX platform environment running Windows 2003 Server and OSX Server, including VPN, SW/HW, network support & security in Windows 2003 Server & Mac OS X Server environment, support of network configurations: LAN, WAN, wireless, VPN. Third level support Tier III, including issue, conflict and management resolution IT Administrator entire Mac/PC Network - Berkeley, CA January 2001 to September 2004 CA Volunteer IT Coordinator and volunteer at Nascent Project, a non-profit corporation, designed to assist at risk youth by offering new skills, workshops, and skill shares. Projects promoting bio-diesel usage and environmental efficiency, and traveling multi-media road shows are some of the educational activities, Administrator and support for entire Mac/PC Network for over 3 years Education M.A. in Ethnomusicology in Ethnomusicology California State University 2003 to Present Information Security Professional City College of San Francisco - San Francisco, CA September 2008 to March 2010 Educational Technology, teaching San Francisco State University 1994 to 1998 design Institute of Technology - Vancouver, BC 1996 B.A. in Liberal Studies California State University 1993 Skills Lamp, Security, Aix, Apache, Linux, Solaris, Unix, Dlp, Nessus, Nexpose, Pki, Qualys, Splunk, Cisco, Encryption, Firewalls, Networking, System administration, Virtualization, Ipv6 Additional Information Supervised, trained, and managed new staff & implementation of support departments -Ability to manage several projects simultaneously -Dependable, flexible team member; advocate -Experienced troubleshooter, IT support & IT security consulting -Bilingual in English and Spanish Computer Proficiency: -Proficient in UNIX (OSX Darwin, AIX, Solaris, Linux-CentOS, Ubuntu, Debian); securing, hardening & compliance -Experienced in-Python, AppleScript, HTML, Apache, Cisco Internetworking; -Palo Alto Networks firewalls enterprise deployment; PAN CLI -QRadar, Splunk, Nessus, Qualys, OpenVAS, Nexpose, AlienVault , Exabeam, Symantec Endpiont, Symantec DLP- use and management of security tools -Experienced with encryption methodologies and PKI -Experienced in network support, system administration, security, penetration testing, scripting -Administration of LAMP servers, logging, monitoring, maintaining, metrics, automation -20 Years of desktop & network support experience in Windows & Mac client environments -Proficient in Windows 95-Windows 10, Mac OS X & Linux platforms incorporating business, design, networking,

administration, security and testing; trained in IPv6 -Audio, video and multimedia applications; hardware, software & peripherals included, MIDI -Virtualization (Vmware, Virtualbox, Rackspace, AWS, Eucalyptus, Citrix Xen) -Cloud security- Security and Privacy, Compliance, and Legal/Contractual Issues; AWS best security practices in EC2 and RDS -OWASP & WASC advocate and administrator of testing and methodologies

Name: Marcus Young

Email: ngonzalez@example.org

Phone: +1-725-756-7595x392