Marco Mancia

**C.510.407.1849**

**Oakland, CA**

[marco@spaz.org](mailto:marco@spaz.org)

**Career Objectives**: 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

# **HIGHLIGHTS OF QUALIFICATIONS**

-Supervised, trained, and managed new staff & implementation of support and SOC departments

-Ability to manage several projects simultaneously

-Dependable, flexible team member and team lead

-Experienced troubleshooter, IT support & IT security consultant

-Bilingual in English and Spanish

**Computer Proficiency**:

- Proficient in **UNIX/Linux (OS X, Darwin, AIX, Solaris, Linux-CentOS, Debian-Ubuntu, Kali)**; securing, security testing, hardening & compliance

-Experienced in–**Python**, **AppleScript, HTML, Apache, Cisco Internetworking;**

**-Palo Alto Networks** firewallsenterprise deployment; **PAN CLI**

**-QRadar, Splunk, Nessus, Qualys, OpenVAS, Nexpose, AlienVault, Exabeam, Symantec Endpoint, ExtraHop, Microsoft Sentinel, Symantec DLP–** use and management ofsecurity tools

-**ServiceNow** proficient

-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, Eucalyptus, Citrix Xen)

-**Cloud Security-**Security and Privacy, Compliance, and Legal/Contractual Issues; **AWS** best security practices in EC2 and RDS; security configurations, vulnerability testing and security posture assessments

**-OWASP & WASC** advocate and administrator of testing and methodologies

-**AWS Certified Cloud Practitioner**

**-Microsoft Sentinel** trained

-**Mac** and **OS X** Certified support/admin professional and trainer; Mac support technician and support engineer since 1994 up to current **macOS 12 Monterey** and new USB-C macs,

specializing in troubleshooting, administration, enterprise rollouts, **JAMF**, MDM, Data Recovery, networking compatibility, and access and compatibility within **Windows/Linux** enterprise environments; security assessments, OS X and server hardening, monitoring and upgrade efficiency; executive level support for C-Level at **Fluidigm (exclusive for the CEO), Blackhawk Network, BlueShield, Prospect Sierra Middle School, Pivotal Labs, Groundwork OpenSource, Publicis Re:Sources, UCOP, The Nascent Project and techNotics LLC**

**Experience:**

**Highlights of recent engagements:**

**T-Mobile-(Security Consultant) - short term project for traffic validation to new security devices & Log4j vulnerability assessment and remediation)**

**(January 10-Feb 5th 2022)-**Assessment of all Java applications jndi output; manual testing by using scripts to test the jndi output; as well as the log4jce script scanner tool, and **InsightVM** vulnerability scanner; **Crowdstrike’s** log4j tool as well; also testing of all Microsoft applications that were using log4j elements; remediation consisted of advising the system admin/operations teams on what versions to upgrade to or bypasses to use; also headed traffic validation from **Gigamon**’s to new traffic routes and new security devices, from the Sprint transition overhaul, testing of **Cequence** bot detector for deployment and for IR-SOC, configuration & testing of **Imperva** WAF for internal and external sites

**First American Title -**[**firstam.com**](http://firstam.com/)**- (July 12 to November 5, 2021) – Sr. Security**

**& Cloud Deployment Engineer-**On a short term project through Deloitte for Internationally known title company; main emphasis on deployment and tuning of ExtraHop in On-Prem environment and AWS and Azure; daily threat monitoring and hunting using [**ExtraHop**](https://www.extrahop.com/), [**Intsights**](https://intsights.com/), [**Tanium**](https://www.tanium.com/), [**Splunk**](https://www.splunk.com/), [**Vectra**](https://www.vectra.ai/)**,** [**Windows Defender**](https://www.microsoft.com/en-us/windows/comprehensive-security)**;** architecting of solutions, and lead on security & project tools deployment; Project lead for ExtraHop deployment in over 7 data centers around the country, including 2 in India, and 2 in AWS & Azure environments all within 4 months

**BlueShield of California (Nov. 30 2020 to July 2021) – Sec Engineer-**project for Blue Shield; admin and detection analyst for **FireEye HX** and **NX**; **Splunk** efficiency for incidents and forensics knowledge; [**IBM** **Resilient**](https://www.ibm.com/security/intelligent-orchestration/soar?p1=Search&p4=43700050370322228&p5=e&gclid=EAIaIQobChMIn9Gxoseu8gIVXgytBh0QwA8cEAAYASAAEgIZE_D_BwE&gclsrc=aw.ds) SOAR incident implementation; Symantec DLP integration and policy tuning; **Proof** **Point** TLS partner implementations; admin and main escalation point for scanning environment using **Tripwire IP360 and Tenable.io** in multi data center, cloud and on-prem environment of a total of over 10,000 assets**;** creator of threat hunting program to help the organization assess their security posture in their prospective industry, along with partner affiliations and industry verticals

**Zillow Group, Inc. (Mar.16-Sep.22, 2020) in a contract role as a Security-IR Engineer);** Tier 1-3 incident Responder/SOC engineer for Zillow Group and all its affiliates, monitoring & alerting of all tools alerts seen in **FireEye** Helix, **0365** Threat tools, **Okta** logs, **Umbrella**/OpenDNS/Kibana, Squert, Suricata, **Splunk**, **CrowdStrike**, **Meraki**, AWS **GuardDuty**, AWS **CloudTrail**; AWS security best practices and procedures; tuning of tools and increasing efficiency of alerting, initialization of automation in SOC operations and helping encompass Managed Security Services for a vendor implementation (Optiv); have helped increase response times for incidents to 25%; integral part of security engineering projects in deployments, advising, consulting, communications, and inclusive engagement with fellow infrastructure, operations and dev teams

**PG&E (4 week assignment Jan 2020 to Feb 2020-on leave fill in)-Tenable Nessus SME-**Administrator and security engineer for Tenable Security Center and Nessus Manager; unique enterprise deployment unlike any other organization; tuning of Nessus scans, large array of scheduled scans, multiple scanners across the enterprise, testing of large subnets, multiple domains, weekly tuning for efficient and high value vulnerability scanning; with over 14 million assets scanned every week; support engineer/sysadmin for technical issues; increased number of found Assets by 65%, and patching time down by 25%

**Fluidigm (April 2019 to present part time consultant)-IT Security/Administrator/Incident Management/Red teamer-**Security Operations, Response and Solutions, 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

**Blackhawk Network Holdings (Feb-2018 to Feb 2019) – Staff Security Engineer –** 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

**Adhere, Inc. (Sep to Dec. 2017) – SOC Engineer II/Penetration Tester –** Audit, Regulatory & Compliance firm, 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 vulnerability research, threat research & intelligence for tools and process implementation

**techNotics (April 2016 to Aug 2017) –** Private clients for owned company, **techNotics**, including incident response, 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 assets, 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: Typo squatting, DDos, Amplification attacks, resolver attacks, cache poisoning, 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**](http://gap.com) **(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-September 2015) -**Security assessment, incident response, engineering, consulting, solutions & security management; SSAE 16 SOC 1 compliance assurance

[**Riverbed Technology**](http://files/Content.Outlook/8ENNH4OX/riverbed.com) **(September 2014- January 2015) -Security analyst & 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

[**VMware**](http://files/Content.Outlook/8ENNH4OX/vmware.com) **(March 2014 – August 2014)** - **SOC** **Analyst** using **NetWitness**, **zScaler** and **Splunk** for malware/DDos/forensics/botnet detection for their SOC; incident responder Tier 1-3, triage for any incidents, investigations, memory analysis, and support for remediation to prospective teams

**The Gap, Inc (March 5, 2012-January 2013-) - Sr. Security Engineer,** 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

**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:**

**October 1994-present-**(Owned business)–[**techNotics.info**](http://technotics.info/)**,** Sr. Researchist & Consultant, IT Support & Security, Bay Area, 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

**Sep. 2014 – January 2015-Riverbed Technology-**Information Security Analyst 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; creation of SOC and Incident Response program; and internal pen testing process

[**The Gap**](http://gap.com) **(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

**Sep. 20, 2011-December 2011-Sephora, Inc-** Security Systems Engineer, 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);**

**July 5, 2011-August 8, 2011 -Groundwork OpenSource-** Support Engineer, Support 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](http://gwos.com/)

**September 2010-December 2010-Pivotal Labs, Inc**. Operations Engineer, - 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](http://pivotallabs.com/)

**June 2010-February 2011** -**Xobni**, Inc. – Technical Support Engineer – 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](http://www.xobni.com/)

**April 2010-June 2010-Yahoo!-**Mail Security Engineering Analyst, Anti-Spam analyzing, honeypot network creation, projecthoneypot.org collaboration, account seeding, tracking and logging; succeeded on making their webmail spam filter more efficient by 40%

**December 2009-April 2010** -**NeuroFocus**, Inc. – Systems Specialist, System Administration, Network Administration and workstation support 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](http://www.neurofocus.com/)

**February 2009-December 2009 -Prospect Sierra Middle School –** IT Administrator, 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](http://prospectsierra.org/)

**October 2007-October 2008 –Publicis-re:Sources,** Senior Analyst, San Francisco, CA

-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 directory

Administration, VMWare Manager, Oracle VirtualBox, Ubuntu KVM, Ubuntu Enterprise Cloud

**October 2004-October 2007 –Univ., Calif. Office of the President,** IT Specialist, Oakland,

-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

**January 2001-September 2004 –The Nascent Project**, IT Administrator Berkeley, 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:**

**City College of San Francisco, CA-**AdvancedEthical Hacking & Network Defense, Fall **2008**

**Information Security Professional**: **CISSP** curriculum and training - **Spring 2010**

**City College of San Francisco, CA,** Ethical Hacking & Network Defense course, **2007**

**California State University, East Bay,** Pursuing M.A. in Ethnomusicology, **2003**

**Peralta Community Colleges**, Courses in **UNIX** and PC Repair & Support, Oakland, CA, **1997**

**San Francisco State University**, Graduate course work in Educational Technology, teaching assistant & intern in the Multimedia Studies Program for over 4 years, **1994-1998**

**DigiPen, Institute of Technology**, 2-D & 3-D Video Game Programming, Interface design, C Programming-Vancouver, B.C., Canada, **1996**

**California State University, Northridge**, B.A.-Liberal Studies, Minor-Anthropology, **1993**

**Training:**

**LearnIT! –** Windows Server 2003 & Active Directory Course, certified for **MCSE, 2007**

**LearnIT! –** Windows Vista for IT Professionals**,** certified for **MCTS, 2007**

**LearnIT! –** Dreamweaver Intensive**,** eligible for certificate, **2007**

**North American Computer College**  
Glendale, CA, USA   
Completed course in Linux GNU Certification, **2001**

**ICTP – International Consortium of Technology Professionals**  
Irvine, CA, USA   
Completed courses in Windows 2000 & Server Administration; Linux install & Admin, **2000**

**EdNet**   
Woodland Hills, CA, USA   
MCSE Program Courses completed in DOS & Networking Essentials, **1998-1999**



**Certification Achievements:**

**ExtraHop** Essentials Certified

**AWS Certified Cloud Practitioner**

Member of **ISSA-Information Systems Security Assocication**

**C**isco **C**ertified **N**etwork **A**ssociate (**CCNA**)

**CISSP** trained

**CEH (**Certified Ethical Hacker**) 2007**

**Palo Alto Networks Admin & Security** certified

Member of **Pentester Academy**-[securitytube.net](http://www.securitytube.net)

Member of eLearning - <https://www.elearnsecurity.com/>

**A+**, **Network+, Security+, Linux+** certified

**M**icrosoft **C**ertified **P**rofessional, **MCP**

**ACSA, Apple Certified System Administrator**

Achieved **Apple Product Professional** status 1998-2006

Completion of four courses in **MCSE** track

**ITIL** certified, Feb. 2008

**IPv6** trained

Yearly attendant of **Black Hat**, **Defcon**, **bsides** and **baythreat.org** conferences

Strong **Agile** & **Security** advocate

Experienced in non-profit creation & grant writing

Fluent in **Spanish**

**Affiliated & supported websites:**

[http://technotics.info](http://technotics.info/)

[http://www.holdfastrecordings.com](http://www.holdfastrecordings.com/)

[http://www.spaz.org](http://www.spaz.org/)

<http://katabatik.org>