Security Architect Security Architect Security Architect - F&A Consultants Detroit, MI I have 10+ years of experience in Systems, Network and Application Security domain with a team player attitude and problem-solving approach. I have worked on both sides of Information Security spectrum i.e. Offensive as well as Defensive Security. I am subject matter expert (SME) for Symantec security solutions. I have designed, deployed and provided support for enterprise security solutions like: Data Loss Prevention (DLP) Encryption Endpoint Protection Data Center Security (DCS) Messaging Gateway (SMG) Intrusion Prevention System (IPS) Web Application Firewall (WAF) Privileged Access Management Secure Web Gateway (SWG) On Security Assessment side, I have successfully delivered many Penetration Testing and Vulnerability Assessment projects. Major highlights of career include: Architecting and deploying enterprise security solutions. Large scale Data Loss Prevention (DLP) projects Conducting Penetration Testing (PT) and Vulnerability Assessment (VA) Writing Security documentation like Solution Design, Penetration Testing Reports, Rules of Engagement (ROE), Technical Proposals, Statement of Work (SOW), Pre-Engagement Questionnaire etc. Experienced in training and implementation of ISO 27001 and ISO 22301. Work Experience Security Architect F&A Consultants - Detroit, MI October 2017 to Present Working with clients like State of Michigan, Blue Cross Blue Shield of Michigan (BCBSM). Designing and implementing Information Security solutions in a highly complex and large environments. Implementing Enterprise Log Management with Syslog-ng/QRadar, Enterprise Vulnerability Management with Tenable SCCV. Identifying security requirements for applications, services and supporting infrastructure and communicating requirements to application development teams and project teams. Reviewing static and dynamic application security assessment reports and consulting with developers for remediating vulnerabilities. Senior Information Security Consultant PCM - El Segundo, CA June 2015 to September 2017 Provided Information Security consultancy to US clientele that included Bank of Guam, Sturm Ruger, Citizen Security Life, Madison Resource Funding, USI Insurance, YUM-KFC, Syros Pharmaceuticals, Radford University, Modern Health etc. Acted as Subject Matter Expert for Symantec's security solutions. Day to Day administration of PCM's Symantec Endpoint Protection

(SEP) Infrastructure consisting of around 5000 clients in USA, Canada, Philippine and Pakistan. Upgraded and consolidated En Pointe's and PCM's Symantec Endpoint Protection (SEP) Infrastructure after PCM's acquisition of En Pointe. Audited Sturm Ruger's existing Symantec Endpoint Protection (SEP) deployment and identified weaknesses in policies and security settings. Designed and deployed Symantec's File Share and Endpoint Encryption solutions for Bank of Guam. Provided Technical support and demo for Symantec Data Loss Prevention (DLP) to existing and potential clients like Citizen Security Life, Madison Resource Funding, USI Insurance etc. Upgradation of Sturm Ruger's Symantec Endpoint Encryption (SEE) Infrastructure. Providing consultancy and Technical support for Symantec Data Loss Prevention, Symantec Endpoint Protection (SEP), Symantec Endpoint Encryption, Symantec Data Centre Security (DCS), Symantec Messaging Gateway Wrote security documentations critical to success of Project like Penetration Testing Reports, Rules of Engagement (ROE), Proposals, Statement of Work (SOW), Pre-Engagement Questionnaire, Solution Design etc. IT Security Analyst Security Operations in Middle East and South Asia July 2013 to December 2014 Lead Penetration Testing and Vulnerability Assessment projects for number of clients in Gulf and South Asia. Lead team of eight (8) security engineers, the team was responsible for Security Operations in Middle East and South Asia. Deployed and configured Trustwave Web Application Firewall (WAF). Acted as a Technical lead and successfully completed the project of acquiring McAfee Next Gen IPS (NS9100) for the ISPs to deploy in their primary and backup Datacenters. This includes Planning, Deployment, Configuration and technical support Conducted several trainings for Lead Implementer ISO 27001 (ISMS) and ISO 22301(BCMS) for company employees and clients. Delivered CEHv8 training to in-house Info Sec team. All 8 engineers who attempted CEHv8 exam passed after training on first attempt. Conducted Account Management tasks for Symantec, McAfee, SourceFire, TrustWave, and DeviceLock. Delivered EC-Council's Accredited Certified Ethical Hacker (CEH) v8 training as an instructor (CEI) to students in Kuwait. Wrote security documentations critical to success of Project like Penetration Testing Reports, Rules of Engagement (ROE), Proposals, Statement of Work (SOW), Pre-Engagement Questionnaire, Solution Design etc. Conducted Security

Awareness seminars for general public to educate them about Penetration Testing and critical vulnerabilities of that time like Heartbleed etc. Security Engineer ABM Info Tech - Islamabad, PK April 2012 to June 2013 Designed, Deployed & Configured Symantec Data Loss Prevention (DLP) at Zong (A mega Telecommunication Provider with more than 31 million subscribers). Deployed & Configured Symantec Data Loss Prevention (DLP) at Ufone (A large Telecommunication Provider with more than 20 million subscribers). Deployed and provided support for Dell Quest Total Privileged Access Management (TPAM). Designing and Planning of Symantec Data Loss Prevention (DLP) for Election Commission Uganda. Delivered Proof of Concept (POC) of Symantec Data Loss Prevention (DLP) to Securities & Exchange Commission of Pakistan (SECP) Successfully conducted Proof of Concepts (POC) of Symantec Messaging Gateway (SMG) for Higher Education Commission (HEC) which was providing email service to more than 60 universities in Pakistan. Provided consultancy and support for Symantec Endpoint Protection (SEP), Symantec Critical Systems Protection (CSP), Symantec Messaging Gateway (SMG), Symantec Web Gateway (SWG) and Symantec Security Information Manager (SIEM) Technical Executive NOC Wi-tribe - Islamabad, PK November 2011 to March 2012 Operation & Maintenance, Troubleshooting of Cisco Metro Ethernet ME3400 Access Switches & Cisco 7600 Gateway & Aggregation Routers. Configuration and monitoring of DHCP services on CentOS and Solaris Server. Monitoring of network serving 100k+ subscribers with MRTG, HP Open View NAGIOS, Motorola & Huawei EMS & NMS etc. Information Security Officer MTBC - Rawalpindi, PK March 2011 to August 2011 Performed Penetration Testing (Application) to detect any vulnerability and weakness that could have been exploited by malicious hackers and fixed the identified problems with relevant teams. Many critical level vulnerabilities were identified during Penetration Tests which was lauded by the Senior Management. Identified vulnerabilities included clear text FTP passwords, clear text Network Firewall password, eavesdropping on voice calls using MITM, exfiltration of sensitive information containing PHI using steganography etc. Reviewed access logs and reported anomalies in the operating system, database, network, applications and made sure company's Information security posture was in compliance with HIPAA regulation. Blocked all types of Portable Device Access of employees with GFI Endpoint Security. IT Consultant Freelancer - Islamabad, PK January 2010 to February 2011 IT Consultant Installed, configured and administered Cisco Routers, Switches, Windows Servers 2003/2008 and Red Hat Enterprise Linux Servers. Conducted Penetration Testing and Vulnerability Assessment. Teaching Assistant FAST-NU - Islamabad, PK January 2008 to May 2009 Assisted graded, provided consultations to the student and managed student projects. Conducted the labs of programming courses (Introduction to C/C++, Object Oriented Programming, Operating Systems etc.) in which students were taught practical aspects of the course. Taught students C/C++ programming on Visual C++ and Linux. Education Bachelor of Engineering in Telecommunication Engineering National University of Computer and Emerging Sciences - Islamabad, PK Skills Security, Websense, Data loss prevention, DLP, IPS, Information Security, Cyber Security, SIEM, Nist, Network Security Additional Information COMPUTER EXPERIENCE SUMMARY: Technology Product Endpoint Protection Symantec Endpoint Protection (SEP), GFI Endpoint Security Data Loss Prevention (DLP) Symantec Data Loss Prevention Messaging Gateway Symantec Messaging Gateway (SMG) Web Application Firewall Trustwave WAF Encryption Symantec Endpoint Encryption (SEE), Symantec Drive Encryption, Symantec File Share Encryption, Advanced Threat Protection (ATP) Symantec Advanced Threat Protection Data Center Security Symantec Data Center Security (DCS), Critical System Protection (CSP) Web Gateway Symantec Web Gateway (SWG), Microsoft ForeFront TMG, Websense Intrusion Prevention System (IPS) McAfee Next Generation Intrusion Prevention System (NGIPS), Source Fire Intrusion Prevention System Log Management Syslog-ng, QRadar Privileged Access Management Dell Quest Total Privileged Access Management (TPAM) Activity Tool Port Scanning and Foot Printing NMAP, Hping3, NetCat, Google, Tor Vulnerability Assessment Nessus, Acunetix, Retina, AppScan, Qualys, OpenVAS Exploitation and Attack Metasploit, Cain & Abel, Ettercap, sslstrip, L0phtCrack, Burp Suite Sniffers Wire Shark, Dsniff, Tcpdump Skills Details Microsoft OS Windows 98/2000/XP/Vista/7/8/10, Windows Server 2003/2008/2012/2016 Linux OS Red Hat Enterprise Linux, Cent OS, Fedora, Ubuntu, Back Track, Kali Linux Languages C/C++, SQL, Python, BASH, PowerShell, JavaScript

Name: John Terrell

Email: matthew18@example.net

Phone: +1-624-491-8474