

JULIO R. MARTINEZ

• juliormartinez@msn.com

INFORMATION SECURITY ENGINEER

Accomplished Security Engineer with 30 + years of proven experience and successfully in achieving and exceeding company goals and objectives. Set goals, establish priorities, manage resources, and develop strategies. Mr. Martinez thorough his career was able to communicate through training both technical and non-technical personnel in the use and application of computer based business, administrative support applications and network applications. As an Information Security Specialist Mr. Martinez's responsibilities include:

1. Conducting IT Forensic investigations with Encase and FTK, data spillages, data recovery, and audit logs reviews.
2. Responsible for recommendations and developing of procedures for litigation readiness, E-Discovery Program Development, assisted on training effort. Conduct PII searches activities associated with HIPAA, Sarbanes-Oxley, and PCI compliance. Conducted Litigation email, PST and E-vault archive searches. Experience with several tools for Case Management and Tracking Administration.
3. Lead in all stages of the Vulnerability Management Program to develop and coordinates efforts with other Units to identify and discover security risks. Performed scans within multi-platform networks across enterprise.
4. Conduct Network Security Assessments including Vulnerability Assessments, Threat Risk Assessments, Forensic Reviews and Security Audits. Performed reviews and analyzed source of virus attacks through incident handling, malware analysis, data analytics.
5. Assists in addressing to compliance issues in regulations and standards by reviewing and monitoring security incidents, to help mediate security policy violations, risks correspondence, and reducing human errors by recommending appropriate steps to make individual systems to be in compliance.
6. Experience with usage of several searching tools such as Clearwell appliance, Discovery Attender, Symantec E-Vault, DT search, Hurricane Search, Efficient file search, File Network Locator, Exchange Permission Mgr.
7. Experience with endpoint security solutions for application whitelisting; application blocking, HIPS; antivirus, DLP with Symantec Endpoint, E-sentinel, FireEye, SourceFire, HBSS, AppLocker.
8. As a network engineer provide engineering support for firewalls, routers, IDS/IPS, VMware and Hyper-V to analyzed security risk, and harden appliances based on security policy specifications. Posse's solid Brocade fabrics with enterprise SAN level design/architecture.

U. S. Department of Homeland Security(DHS) Top Security Clearance, 2014 (Active)

U.S. Department of Defense (DOD) Top Security Clearance with Full Scope polygraph, 2010 (Active)

CORE COMPETENCIES

LAN Administration • Network Engineering • Network Security • System Administrator • WEB Master • Helpdesk Specialist • Multimedia and Video Conference Specialist • Telecommunication Specialist • Litigation and E-Discovery Engineer • Customer care and Service • Customer care and Service • Customer care and Service • Team Building & Leadership

PROFESSIONAL EXPERIENCE

JME - Information Security Engineer Principal – Chantilly, Virginia (2019 – Present)

- As an IT Security provide and ensure that the developer source code are analysed and it adheres to any up to date coding standards for the language, operating system or platform. Able to inspect all source code on a line-by-line basis, reviewing authorization, authentication, session and communication protocols for security. As part of the analysis, penetration testing may be required to help confirm vulnerabilities present in the code. In addition work as a source code auditor to assist the development team to prepare code for the auditing process. Perform investigative task on a source codes to identify all the spots of the code where sensible information could get leaked through to preventing any unauthorized access. responsible of preparing and maintaining engineering and security related documentation. Conduct technical and nontechnical reviews and

audits as necessary to support C2S (AwS)m Hybrids, and onprim development. Assist system administrators and ISSM in maintaining system accreditations in accordance with the approved IA program and procedures.

.Leidos - Information Security Engineer Principal – Reston, Virginia (2018 – 2019)

- Provides support the Information Assurance (IA) team (ISSM, ISSO), system administrators, and program technical staff for ongoing and emerging programs requirements. Responsibilities include implementing Information Assurance and Information Security protections and requirements in program development and execution environments. Duties will include performing analysis, identifying and implementing protection solutions, and preparing and maintaining engineering and security related documentation. Perform vulnerability assessments; C&A; implementation of security controls in networking devices databases, operating systems, hardware and software components; administering and managing security Plan of Action and Milestones (POA&M) mitigations and POA&M corrective actions; conducting technical and nontechnical reviews and audits as necessary to support C2S (AwS)m Hybrids, and onprim development. Assist system administrators and ISSM in maintaining system accreditations in accordance with the approved IA program and procedures. Prepare documents and provide DOD formatted System Security Plan for C2S Cloud systems and VM Systems.

CSRA/GDIT - Information Security Engineer Principal – Reston, Virginia (2017 – 2018)

- Evaluate designs, tests, and implements secure operating systems, networks, security monitoring and management of IT security systems and applications. Perform security analysis in existing architectures. Conducts risk and vulnerability assessment at the network, system and application level. Develops and implements security controls and formulates operational risk mitigations along with assisting in security awareness programs under RMF, CNSS 1253 and NIST 800-53. Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access. Conducts research and evaluates technical performance of software products and overall segments and systems. Prepares security reports to regulatory agencies. Provide support security planning, assessment, risk analysis, risk management, and audits.

Information System Security Engineer- Arlington, Virginia (2014 - 2017)

- Ensuring that Client's applications and infrastructure are designed and implemented to the highest standards. Analyzing system services, operating systems, networks and applications from a security perspective. Assess and identify security issues/risks in order to be mitigated. Participate in security audits, risk analysis, vulnerability testing and security reviews on many elements of the client's systems. Provided VMWare Vcenter, Hyper-V, AD, DHCP, DNS, Symantec EndPoint, splunk, Nessus, Nagios and Archsight support. Responsible for IPS (SourceFire), Malware appliances (FireEye), RedSeal, Tableau, and VMs.

CSC/EA - Information Security Engineer (ISSE), - Annapolis Junction, Maryland (2011 - 2014)

Information System Security Engineer (2013 - 2014)

- Conducted Security monitoring, threat identification, analysis and mitigation. Network availability monitoring and network security monitoring. SIEM Net IQ Sentinel 6 for Monitoring and Correlating events from Firewalls, IDS/IPS, BlueCoat, Websense content filtering, HIPS and HBSS (McAfee), Systrak. Created search correlation, Filter and Report scripts based on Sentinel Taxonomies. Responsible for discovering, assess and meet Endpoint systems security protection needs, defining requirements, design, develop, implement, evaluate their security architecture. Successfully managed all aspects of IT risk, analysis, and compliance base on DCID/6/3, NIST800-53, HIPPA, COBIT.

Security Compliance Specialist (2012 - 2013)

Storage Area Network Specialist (2011 - 2012)

Security Compliance Specialist (2012 - 2013)

Continued...

TKCCommunications - Information Security Analyst - Washington DC

(2009 - 2010)

- Mr. Martinez has been working with the Security Division to provide the services needed for the DOJ/FBI DOJ regulatory compliance of Vulnerability Management Program (VMP). In addition, he is still responsible for addressing security incidents such as virus outbreaks, conducted Forensic discoveries, data spills contentions, data collection for litigations requests.

BAE Systems Inc. - ITS Security/System Admin/ Sr. Network Engineer - Washington DC

(2004 - 2009)

Information Security Analyst - December 2006 – September 2009

- Worked with the Security Division; he is responsible for conducting security assessment of client's environment to ensure DOJ regulatory compliance of Vulnerability Management Program (VMP), E-Discovery and Forensic Analysis.

Senior Network Engineer - April 2005 – December 2006

Sr. Principal System Engineer - August 2004 – April 2005

ITEQ Inc. - System Administrator, Firewall Specialist - Washington DC

February 2003 – July 2004

TWD & Associated Inc. - System Administrator - Washington DC

June 2002 – August 2002

Planning Consultants Inc. - Network Administrator - Crystal City, VA

July 1998 – August 2001

FOSS NIRSystems Inc. - Network Administrator - Silver Spring, MD

January 1995 – April 1998

Perstorp Analytical Inc. - Field Service Electronic Engineer - Silver Spring

January 1986 – December 1994

EDUCATION

- **Master of Science**, Network Security, Capitol College, 2002
- **Bachelor of Science**, Computer Engineering, Capitol College, 1997
- **A.A. Science**, Computer Draft Engineering, Montgomery College. 1983
- **A.A. Science**, Computer Science, Montgomery College, 1982
- **A.A. Science**, Civil Engineering, Universidad Nacional de Ingenieria, Lima PE, 1975

TRAINING

- **AWS DevOps – Montgomery College - 2019**
- **Security Operations on AWS – AWS 2018**
- **Amazon Web Services (AWS) Fundamentals – Montgomery College - 2018**
- **Xacta 365 User Training– Telos – 2017, Xacta Continuum User Training– Telos – 2018**
- **Searching and Reporting – Splunk University Education - 2016**
- **RedSeal Fundamentals – RedSeal Network - 2015**
- **IPv6 Implementating the Next-Generation Network - The Learning Tree – 2015**
- **Microsoft Azure Infrastructure Services - The Learning Tree – 2015**
- **XACTA, and Applied Security Engineering Methodology ASEM – DOD-2014**
- **HP Fortify: SAC,FOD,WAB,WebInspect – HP- 2014**
- **SysTrack Resolve – Lakeside – 2014**

Continued...

- **E-sentinel** Administration & Development – Novell -2014
- **Oracle Solaris** System Administration – Training/etc Inc. - 2013
- **Social Engineering Deceptions and Defenses** - The Learning Tree – 2013
- **Preparing for the CISSP** - The Learning Tree – 2013
- **ITIL Foundations v3** - PeopleCert – 2012
- **MS SQL 2008 R2 Administration** - ACE - 2012
- **VMware vSphere: Install, Configure, Manage V5.1** – VMware – 2012
- **First Line Leadership Courses** - BAE – 2009
- **Windows PowerShell Hands-On: Automating Administrative Tasks** – The Learning Tree – 2008
- **Implementing and Troubleshooting Wi-Fi Networks** – The Learning Tree – 2008
- **ScriptLogic** Administration suite - Accelera – 2007
- **Ethical Hacking and Countermeasures, Computer Forensics and Incident Response, Vulnerability Assessment** - The Learning Tree – 2007
- **CCNE** Cisco – Montgomery College – 2003,
- **Stone Gate Firewall** – TrueNorthSolutions, Citrix ThinNet Client - Network Resources – 2002

CERTIFICATIONS

- Electronics Technology Certificate, HumRRO Tech, Washington DC, 1983
- CCNE Cisco – 2003,
- Comptia Security Plus - 2013
- ITIL Foundations v3 – 2012
- ScriptLogic Administration suite – 2007
- Computer Forensics and Incident Response – 2007

TECHNICAL EXPERIENCE

Applications

- Encase and FTK
- Network drawing software: Net Wiz, Pinpoint and Visio.
- Government Applications Software: FMIS, CMDS, AEGIS, ACSESS CMS.
- Software:Hp Fortify, Webinspect,NESSUS,Retina, Nmap, wireshark, FoundStone, Network-1, Raptor, RedSeal, E-Sentinel,Observer Network monitoring, TCP/IP tools Stats, security, Security Expression, Nat32, Black Ice Defender, Iscan – Trend Mail and SysTrack VDI Monitoring (Lakeside),AppDetective.
- Spam/Filtering: Symantec Exchange/Virus/Spam/Filter Agent, Mail sweeper- Sweep Mine, Iron Mail, Web Monitoring: from ON Technology, Log Analyzer from Web Trends, Surf control. Quest Suite Products.

MILITARY SERVICE

- United States Marine Corps Reserve, June 1978 – June 1982