Luis A. Arana

**GOAL ORIENTED SECURITY PROFFESIONAL**

*Highly* ***qualified*** *security professional with over twenty years of technology and security experience in both the federal and private sector.* ***Outstanding*** *managerial and interpersonal skills resulting in effective customer working relationships and top return on investment.* ***Proven*** *problem solver that accurately assesses technical challenges and successfully transforms ideas into* ***secure*** *solutions. Expertise and capabilities include:*

|  |  |
| --- | --- |
| * ***Systems Auditing*** | * ***Network Security*** |
| * ***Risk Assessments*** | * ***Certification and Accreditation*** |
| * ***Problem Solving*** | * ***Security Tests and Evaluations*** |
| * ***Subject Matter Expertise*** | * ***Team Building and Leadership*** |
| * ***Project Management*** | * ***Research and Analysis*** |

**QUALIFICATIONS HELD**

|  |  |
| --- | --- |
| * CISSP- Certified Information Systems Security Professional * SSCP - System Security Certified Practitioner * CRISC – Certified in Risk and Information Systems Control * GIAC /GSNA - Global Information Assurance Certification: System and Network Auditor | * FITSP: Auditor– Federal Information Technology Security Professional / Auditor * Access Data Certified Examiner * LunarLine Certified Expert Independent Assessor * MCSE+Sec - Microsoft Certified Systems Engineer+ Security (legacy) * CCNA - Cisco Certified Network Associate (expired) * COMPTIA Security +, A+ |
| **Committee on National Security Systems (CNSSI) Certificates:** | |
| * CNNSI 4016(A) – National Information Assurance Training Standard for Risk Analyst (Advanced) * CNSSI 4012 – Senior Information Assurance Systems Manager * NSTISSI 4011 – Information Systems Security (INFOSEC) Professional | |
| **Security Clearance: Top Secret / SCI Status: ACTIVE** 18 years **Adjudicated: June 2016** | |

**PROFESSIONAL EXPERIENCE**

#### C4 Planning Solutions LLC, *Miami, FL*

***Information Systems Security Officer*** Sept. 2016 – Present

*Supporting United States Army Network Enterprise Center and USSOUTHCOM J6 in network modernization efforts pertaining to risk management and governance.*

* Perform cybersecurity and risk management activities for current network operations as well as the development of cyber governance and risk management activities for network modernization actions for 4 direct reporting units.

***Cybersecurity and Network Defense Project Manager*** Feb. 2016 – Sept. 2016

*Contracted to lead a contractor managed theater cyber and network security operations supporting J6 Communications Directorate for United States Southern Command.*

* Manage the DOD Risk Management Framework (RMF) governance and compliance program for theater components within CONUS, Central and South America.
* Oversee the theater incident management response program comprised of global host intrusion prevention, vulnerability scanning and intrusion detection activities.
* Execute US Cyber Command cyber tasking program for all US Southern Command Direct Reporting Units and agency partners in supporting direct cyber actions in protection of the Department of Defense Information Network (DoDIN); an interconnection of DoD computing enclaves and information systems.
* Develop compliance inspection program following US Cyber Command methodologies and practices for theater-wide components.
* Orchestrate policy development and training compliance practices.

#### X-eeto Incorporated. *Miami, FL* Aug. 2014 – Feb. 2016

***Information Systems Security Officer***

*Supporting 7th Signal Command, 525th Signal Company network operations for Headquarters, United States Southern Command under the J6 Communications Directorate. Charged with the secure management, operation and validation activities of Secret, Unclassified and Commercial networks.*

* Develop and oversee the RMF program for the 525th Signal Company supporting US Southern Command Headquarters as well as site-based accreditations and ensure all systems connected of the network meet all established Federal, DoD and site Cybersecurity requirements.
* Orchestrated continuous reviews of all information systems and networks to ascertain any changes that will negate the accreditation or affect the security posture of said systems and enclaves by conducting threat and vulnerability assessments, technical audits and developed risk assessments of Headquarters and supporting organizations information systems to determine the appropriate measures to manage those risks effectively.
* Responsible for developing and executing security impact and risk analyses as well as authorization activities on all project, platform IT an, partner-nation and commercial communication systems utilizing HQ's computing resources.
* Act as the Cybersecurity project advisor for IT projects and separate procurement actions with responsibility for providing technical and security advice in the information assurance arena.
* Developed policies and procedures to localize all DoD, Joint Staff and CYBERCOM cyber-security regulations.

#### Lockheed Martin IS-GS - Defense. *Miami, FL* Feb. 1999 – Aug. 2014

***Sr. Network Security Analyst / Information Systems Security Officer***

*Recruited to support United States Southern Command’s J6, C4I Security division; supporting computer network defense and certification and accreditation of over 35 military / interagency missions and direct reporting units throughout Central, South America and the Caribbean. Expertly lead the achievement of continued security best practices concerning the securing of information technology (IT) systems within the U.S. Southern Command AOR. These concerned the design and execution of enterprise security management features, and the enactment of government certification mandates and industry best practices for security on all information assets; resulting in an overall security posture improvement of over 95% over a period of fifteen years.*

*Certification and Accreditation (C&A) Accomplishments:*

* Created and validated Defense Information Assurance Certification and Accreditation Process (DIACAP) C&A products to include System Identification Profiles (SIP), DIACAP Implementation Plans (DIP), Scorecards, Plan of Action and Milestones (POA&M’s) and associated artifacts for over a hundred systems throughout the AOR ranging from standalone units, commercial connectivity and SIPRNet/NIPRNet enclaves . Serving under a transition team for NIST RMF, changeover to include schedules and process for the transition of DoD supported systems.
* Expertly interpreted and applied regulations, both DoD, service and agency, in analyzing security controls, and mandates.
* Coordinated and lead assessment teams as principal technical auditor for Information Assurance Review (IAR) and Staff Assist Visits (SAV) for the both the initial and reaccreditation phases of the C&A process on multiple IT platforms, for the commands military missions throughout Central, South America and the Caribbean. Developed audit scripts and executed technical Security Test and Evaluations (ST&E’s), in-depth analysis of network architectures and administrative / engineering interviews supporting DITSCAP / DIACAP / NIST RMF Authorization and Assessment processes. Achieving FISMA compliance ratings of over 95% per year. Efforts have garnered accolades from the Joint Staff J6 and was part of the team to receive a nomination for the National Security Agency’s Frank B. Rowlett Award, the attainment of the 2011 DoD Chief Information Officer award for the top Information Assurance team in the DoD. As well as continued A+ ratings for FISMA compliance.
* Command Information Systems Security Officer with direct support of Joint Task Force Guantanamo Bay, Cuba. This includes all C&A projects including circuit accreditations, NIPRNet and SIPRNet, Commercial Internet Service Provider waiver process through the Defense Security Accreditation Working Group (DSWAG) , as well as joint program managed and locally developed systems. Participated and lead Staff Assist Visit (SAV) to Direct Reporting Units (DRU)’s and Security Cooperation Offices (SCO) within the region for all technical and traditional IA activities.
* Editor and Chief of the SOUTHCOM *Information Assurance Informer* which is a quarterly publication highlighting personal and government information security issues to the command user community. Managed to take a fledgling publication due to lack of manpower and skill-sets and increase readership and interest by 60%.
* Technical Advisory Group member for the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) security instruction sets, Gold Disk / Security Content Automation Protocol (SCAP) auditing and execution tools, and Ports, Protocols and Service Management (PPSM) process. Directed the course of tool usage and adoption of security technologies that influence the DoD.

*Computer Network Defense (CND) Accomplishments:*

* Successfully planned, designed and executed the implementation and installation of network based firewalls *(RAPTOR/VelociRaptor/Symantec Enterprise Firewall*) for Direct Reporting Units (DRU’s), in conjunction with all applicable DISA Security Technical Implementation Guides (STIG’s) for configuration and hardening.
* Provided expert security research and analysis for the AOR incident handling process consisting of firewall / IDS event correlation, network capture analysis, interview of appropriate personnel, partner with network engineering and system administration teams and provide after-action reporting. Utilized findings for the creation of custom firewall and IDS rule-sets for the prevention of future incidents.
* Authored utilities utilizing scripting languages for incident investigation as well as customized scanning policies for *Nessus, ISS, Retina* and other vulnerability scanning tools to search for corresponding vulnerabilities that lead to exploitation.
* Developed scripts to improve auditing and incident handling response time by developing tools that minimized auditing times by 30% and validated incidents with 98% accuracy. Instrumental in tools that assisted the command in detecting compromised system libraries after a reported DoD-wide viral outbreak; this provided the command a quick response capability prior to the release of commercial tools and updated signatures for virus detection and host based intrusion detection systems.
* Performed network penetration tests utilizing both open-source and government off-the-shelf tool-sets in support of command exercise; stress testing security solutions, policies and organizational CND practices. Achieved skill-set validation by the NSA’s Red Team to include an invitation to train in tactics, techniques and procedures (TTP’s) at Ft. Mead Maryland.
* Supported U.S. Cyber Command by coordinating, tracking and reporting on Information Assurance Vulnerability Management (IAVM) alerts and Communication Tasking Order (CTO) compliance to higher headquarters.
* Lead assessment engineer of the Information Assurance laboratory; designed for the Security Test & Evaluation (ST&E) of multiple software and hardware products. This lab allowed for the ST&E, pre-deployment prep and theater support for the commands security posture to include: *Site Protector, Hercules, Sidewinder, HBSS, DeviceLock, TrustedOffice Secure Thin Client and Mobile Armor* end-point encryption. Lab consists of multiple physical and ESXi-based IT technologies including *Windows (2000, 2003, 2008, XP, Vista, 7), Linux* (*Debian, RHEL, Ubuntu*), *SUS, iSCSI, NFS, GSX Server, SharePoint, SQL2005* services running on Cisco *2500-3000* series router and *1900-3500* series switches. Created training modules for auditing and security tools and patch management systems.

*Program Management Accomplishments:*

* Represented the organization by providing direct management support in contract execution, proposal development, business development and retention by representing Lockheed Martin’s interest to USSOUTHCOM and assisting the Program Management team in employee management, client relations, interviewing and training.
* Provided Cybersecurity subject matter expertise in proposal writing and business development efforts for Lockheed sister units in the preparation of proposal and capabilities documentation while keeping abreast of the latest industry and federal cybersecurity trends and mandates.
* Developed ISO27001 plans and serve as program Configuration Manager providing configuration control and auditing for all programmatic and functional program deliverables. Developed a CM repository and issue / change management process to include charring a program Configuration Control Board (CCB).

**Anda GENERICS Inc.** *Davie, FL* April. 1998 - Feb. 1999

***Computer Telephony Systems Manager***

*A subsidiary of ANDRX Pharmaceuticals Inc; a manufacturer and distributor of commercialized generic versions of controlled and immediate release pharmaceutical products. Responsible for overall departmental management; including training, system upkeep, project management, budgeting, vendor relations, documentation, and computer telephony integration. Accountable for all outbound call application development and administration on a Solaris based platform at a 200-seat center for the nationwide pharmaceutical.*

* Successfully assembled the development of the company’s call center in relation to software / hardware design, processes, and procedures for the newly created call center environment.
* Headed the year 2000 compliance testing of 4 *Solaris UNIX* systems controlling two *UNISON* computer telephony branch exchange units.
* Expertly coded UI and data mapping solutions linked to *IBM AS/400* databases for call center operations, both for inbound and outbound projects.
* Partnered with network administrative team on the secure integration of Microsoft *Windows NT* to a mostly *Novell Netware 5.0* network. Due to knowledge of Microsoft security issues was able to increase network services efficiency by 45% while still allowing for secure system availability.
* Developed and maintained a budget of over $30,000 dedicated to facilitate developer and administrative team training and certification requirements, licensing and system modernization.

**Precision Response Corporation** . *Miami, FL.* May. 1996 - April. 1998

***Senior Computer Telephony Systems Engineer***

*PRC is a worldwide provider of customer management and marketing solutions for business to customer and business to business. Oversaw DAVOX operations for South Florida facilities. Responsible for all outbound call application engineering for a 1400 seat call center to include application development, sales production reporting and call management.*

1. Implemented the successful unison of predictive dialing equipment onto a networked environment and AT&T PBX also including application development and integration to a *Sybase SQL* backend.
2. Developed *terminfo/curces* based user interfaces (UI) and data mapping routines utilizing *Solaris UNIX* for call center representative scripts. Employed the use of shell scripts for cross platform data access and syslog storage to data-center.
3. Direct development of computer telephony solutions for AT&T, United Negro College Fund, and United Parcel Service that cross referenced customer databases which allowed for a decrease in printing costs.
4. Collaborated on the implementation of *Checkpoint Firewall-1* solutions in support of facilities totaling 550 networked users on a mostly *Cisco* / *3Com* backend requiring *BGP* modification. Project completed with zero production downtime.
5. Contributed in the management of a mostly *Windows NT 3.5/4.0* network, including services diagnostics, account management and patching. Served the role of security incident handler due to practical knowledge of security issues.

**ITI Marketing Services Inc.** *Miami, FL.* Feb. 1994 - May. 1996

***Team Supervisor / LAN Systems Technician.***

*Midwest provider of nation-wide customer call center solutions. Acquired in 1998 by Apcao Inc.*

* Direct supervision of 20 to 30 customer service representatives in inbound and outbound customer service representatives; providing product and services training, development and support for daily sales activities representing clients from CitiBank, Ford Motors, and Lake Buena Vista productions.
* Transitioned to providing first-line support and configuration of computing assets as part of a small three person technology group. Supporting *UNIX Digital*, Cisco and *Microsoft 3.11, 95* on a Novell network.
* Troubleshoot connectivity and network issues, software loads and upgrades.

**EDUCATION**

**Capitol Technology University, Laurel, Maryland.**

**Degree:** **MS in Information Assurance. Dec 2016**

National Security Agency / Department of Homeland Security Designated Center of Academic Excellence in Information Assurance Education

**Florida International University, Miami, FL.**

**Degree:** **BBA, Management Information Systems. Aug 1999**

Member of the **Information Technology Society**, which provided a forum for technological issues to the university community. Hosted several discussions on computer security issues and career mentoring.

**AFFILIATIONS**

* Information Systems Audit and Control Association (ISACA) South Florida Chapter
* Armed Forces Communications and Electronics Association (AFCEA) South Florida Chapter
* InfraGard Miami Florida
* SANS Auditing Advisory Group

**AWARDS**

* Certificate of Appreciation from the National Security Agency (NSA) Attack, Sensing, Warning and Response Technologies Office (V5) for participation in the development of the Data Mining Comprehensive Capabilities List (DMCCL) 2002.
* Information Assurance Professional of the Quarter. 2004 and 2006.
* Four Star Note for exceptional service presented by Gen. Bantz J. Craddock. Commander USSOUTHCOM. 2006.
* Divisional Certificate of Appreciation for leading the ST&E process for the commands data management plan 2010.
* Divisional Certificate of Appreciation for Year End FISMA “A+” rating for the command. 2010/2011/2012.
* Departmental / Unit Award DoD Chief Information Officer (CIO) IA Award recipient. 2011.
* Lockheed Martin Cyber Security Team Excellence Award for Information Security. 2011
* ISO 27001 Cybersecurity Program Certification. 2014

**TECHNICAL SKILLS SUMMARY**

**Operating Systems:** *Windows (NT, 2000, 2003, 2008, 2012, XP, Vista, 7, 8), Solaris, Linux (System V and Debian), CISCO IOS and MS-DOS.*

**Languages:** *VBScript, Bash, Python, PowerShell, C.*

**Firewalls:** *Symantec Enterprise Firewall, Microsoft ISA, McAfee Enterprise (Sidewinder) Firewall, Checkpoint Firewall-1/NG, Untangle, iptables*

**IPS/IDS:** *ISS Site Protector, Snort / Socurefire.*

**Vulnerability Scanning and Remediation:** *Internet Security Scanner, eEye Retina and Retina Event Manager, Hercules Remediation System, WPSCAN, Flying Squirrel, Nessus / Security Center ACAS / (Assured Compliance Assessment Solution).*

**Compliance:** *Symantec Enterprise Security Manager, SecureWave Security Configuration Management, Vulnerability management System (VMS), Enterprise Mission Assurance Support Service (eMASS), Security Content Automation Protocol (SCAP), Common Vulnerability Scoring System (CVSS)*

**Other:** *Symantec Enterprise AntiVirus,**VMWare Workstation, Server, ESXi, Terminal emulation packages, TripWire , WireShark, Metasploit, Armitage, Core Impact (CORE Impact Certified Professional), Access Data FTK, Host Based Security System (McAfee ePolicy Orchestrator / HBSS) as well other open source security tools-sets.*

**Networking:** *Cisco 2500-3000 series routers and 1900-3500 series switches, 3Com SmartSwitches, NetGear, Vyatta*

**Protocols and Services:** *LAN/WAN/Wifi,* *Extensive TCP/IP experience including DNS, DHCP, SNMP, SMTP, VPN, GRE, IPSEC, SSH, SSL, EGRIP, OSPF*

**Storage:** *iSCSI, NFS*

**Security Compliance Frameworks:** *DoD* *and NIST* *Risk Management Frameworks, DIACAP, DITSCAP,FISMA,* ISO27001*, CoBIT,, RiskIT, PCI-DSS.*