Current TS clearance held, willing to travel, willing to work overseas

MARTIN MACLORRAIN JR

1302 Lincoln Place• New York, NY• martin.maclorrain@gmail.com • 808 489 8889•

SENIOR NETWORK AND SECURITY ENGINEER

Solutions-oriented IT Network and Security Engineer with notable success directing a broad range of DOD IT initiatives while participating in planning and implementation of information-security and IP service solutions in direct support of DOD objectives.

- Track record of increasing responsibility in secure network design, systems analysis and development, and full lifecycle project management.
- Demonstrated capacity to implement innovative security programs that drive awareness, decrease exposure, and strengthen organizations.
- Qualified DOD IAT/IAM III.
- Outstanding leadership abilities; able to coordinate and direct all phases of project-based efforts while managing, motivating, and leading project teams.
- Adept at developing effective security policies and procedures, project documentation and milestones, and technical specifications.
- Knowledge of USG C&A regulations, policies, and processes DITSCAP, DIACAP, JAFAN, NISCAP, NIACAP, DCID 6/3, DCID 6/9, NISPOM Chapter 8.

CORE COMPETENCIES: Network & Systems Security; Vulnerability Assessment; Router and switch configuration; Data Integrity/Recovery; Disaster Recovery Planning; Contingency Planning; Research & Development; Risk Assessment; Cost Benefits Analysis,C4ISR

***Certifications:** A+, Network+, MCSA, CCNA, Certified Homeland Security Level- IV, and CISSP

*** Platforms:** *NIX (Red Hat, HP-UX), Windows 2000/2003

*** Networking**: TCP/IP, ISO/OSI, Ethernet, Token Ring, FDDI, VPN, SSH, PKI,. SSL, DNS, HTTP, HTTPS, FTP, FTPS, IPSEC, SMTP, DNS, DHCP, OSPF, RIP, HSRP, EIGRP, AAA, NAT, HSRP,VMPS Configured Cisco Routers (2500, 3600,3800, 4000,6500) using RIP, IGRP, OSPF, EIGRP,BGP Switches(1900,2900,4500,3550,3560)

*** Government off the shelf:** GCCS-M, TBMCS, NTCSS-Optimize

*** Tools**: Norton Firewall and Ghost, McAfee/Norton Virus Protection Utilities, HP Open View, IBM Tivoli, Tripwire, Snort, Cisco Works, Nessus, eye retina, GFI Languard,G2 sidewinders, pix firewalls, Cisco content engine, EnCase, Remedy, Ethereal/Wireshark, NMAP, Tacacs, Juniper Netscreen, FCC-100, Timeplex, CYZ-10,KWR46,KG194,TACLANE.

PROFESSIONAL EXPERIENCE

NCTAMSPAC, Wahiawa, HI 2008– 3/2009

Regional Information Assurance Manager

Manages a regional team of 10 IAM's and 20 IAO's. Develop, review and evaluate pacific region Information security program, including policies, guidelines, tools, methods, and technologies. Identifies significant actual and potential cyber-security problems, trends and weaknesses. Develops long-range plans for IT security systems that anticipate, identify, evaluate, mitigate, and minimize risks associated with IT systems vulnerabilities. Reviews and evaluates security incident response policies. Reviews proposed new systems, networks, and software designs for potential security risks. Implements higher-

…

level security requirements such as those resulting from laws, regulations, DCI or Presidential directives, and prepares documentation required to comply with such laws, regulations, and directives. Provides expert technical advice, guidance, and recommendations to commanding officer on critical IT security issues. Communicates complex technical requirements to non-technical personnel and prepares and presents persuasive briefings to senior management officials on complex/controversial issues.
Key Contributions:

- Created incident response team
- Successfully developed, drafted and tracked over 30 certification C&A packages.
- Praised by several organizations for command security policies during ST&E visits
- Conducted JVAP on several CDS devices

CJTF-HOA, Djibouti, Africa 2007

Lead Systems Administrator/Network Administrator
Recruited to establish and manage enterprise-wide ip services. Oversee Command wide efforts to identify and evaluate all critical systems. Design and implement security processes and procedures and perform cost benefit analysis on all recommended strategies. Research and evaluate new networking technologies to improve existing infrastructure. Made recommendations and assisted in the implementation of changes to work methods and procedures to make them more effective or to strengthen security measures. Researches and evaluate new technologies relative to network design, operations, management and network security. Managed and coordinates daily activities of Network and System Administrators. Presented options to management for the enhancement of DNS, firewall, modernization of firewalls, and inbound e-mail security and robustness. Handling data network issues in and around sites and providing solutions. Supporting and providing solutions for the support engineer at the remote sites, Maintaining Cisco WAN & LAN gigabit/fast Ethernet networks includes Cisco 3840/ 3660/ 3640 series router, 6500/3550/3560 series switches
Key Contributions:

- Optimized network utilizing NBAR to defend against P2P software and improve performance
- Configured BGP route maps to load balance traffic to various ISP's.
- Created policies and procedures governing incident response.
- Established best practice design to develop templates and documentation to improve operation Procedures

NCTAMSPAC, Wahiawa, Hawaii 2006

Lead Systems Administrator/Network Security Officer

Lead 4 NOC Watch Teams in NIPNET/SIPRNET/JWICS/CENTRIXS operations. Conducted monthly vulnerability assessments. Act as escalation point for NOC watch Teams. Troubleshooting, diagnosis, and resolution of LAN/WAN issues, including, although not limited to, T-1 provider problems, OSPF/BGP routing issues, dial-up access (RAS) concerns, and LAN switch configuration flaws
Key Contributions:

- Monitors logs on network equipment including firewalls, intrusion detection systems, and other edge devices and reports issues.
- Escalation point for routing and switching issues with remote sites.
- Trained 4 NOC watch teams in Intrusion detection ,Incident response and ADNS troubleshooting

PROFESSIONAL EXPERIENCE CONTINUED

- Created bash script to minimize anonymous proxy utilization

IA/Network Operations Engineer, NMCI, San Diego, CA 5/2005 to 10/2006

Analyzed systems requirements in response to business requirements, risks, and costs; evaluated, selected, and installed hardware; and monitored and fine-tuned the systems environment performance.

- Deployed Host Intrusion Detection Systems and Network Intrusion Detection Systems to detect rouge devices and restore network integrity and security.
- Used Tivoli Tec Console and Cisco Works to monitor the NMCI network for connectivity issues and irregular activity; lead technical advisor for NMCI military detachment-training pipeline.
- Met with internal customers to define IT needs and to collaborate on possible solutions.
- Authored numerous Job Qualification Requirements for military personnel.
- Review and maintain configuration standards for network environment
- Discovered and tracked rouge devices

USS TARAWA, San Diego, California 2002-2005

Lead Systems and Networks Administrator/PKI LRA

- Lead a team of 25 Personnel in the administration of IT-21 systems to include NIPRNET, SIPRNET and CENTRIXS-M. Mentored more junior technicians/engineers. Acted as escalation point for more junior technicians/engineers. Mentor and train others in information security in addition to training for other technical groups. Install and maintain security infrastructure, IDS, log management, and security assessment systems. Recognized as local Subject Matter Expert on CISCO Routers and Alcatel switches

Key Contributions:

- Implemented DOD PKI initiative.
- Trained over 20 personnel on *nix based GOTS (GCCS-M/NTCSS-OPTIMIZE/TBMCS).
- Vital to the success of various CND and C4I exercises.
- Optimized shipboard bandwidth utilization using QOS

USS KITTY HAWK, Yokosuka, Japan 1999-2002

Network Technician

Provided comprehensive onsite support for all customers. Created rollover, straight thru and crossover cables as needed. Troubleshoot LAN connectivity problems for over 2500 user network utilizing Ping, tracert and nslookup. Utilized What's up gold and HP openview to monitor network status

Key Contributions:

- Installed over 100 classified and unclassified drops.
- Managed *nix based message system (NAVMACS II)
- Built and maintained Visio documentation of network topology

EDUCATION AND CREDENTIALS

A.A.S in Information technology (MAGNA CUM LAUDE)
TIDEWATER COMMUNITY COLLEGE – Virginia Beach, VA

Bachelor's Degree in Information Technology in progress (Excelsior)

Professional Training

Journeyman network core (NEC 2735) Advanced Network Analyst (NEC 2781) Afloat CND
Computer forensics VOIP Security FIWC IA Toolkit Mcafee Eye retina DOD IA Bootcamp

PROFESSIONAL AFFILIATIONS

Member – Information Systems Security Association
Member-FBI Infraguard