Mario Simon

Cell: (954) 809-4098
mario.simon@platinumitsec.com
https://www.linkedin.com/in/mario-r-simon

PROFESSIONAL SUMMARY

Experienced Systems/Network Engineer with a demonstrated history of working in the Military Industry. Skilled in managing daily operations and providing effective on-the-job training to maintain high-level operations in an enterprise environment. Skilled in Network Administration, System Administration, and Red Team Operations. Knowledgeable and trainable cyber-security certified professional who can learn, apply, and remain versatile to the ever-growing cyber-security and IT industry. Independent thinker capable of supervising work teams of any size to accomplish non-critical/critical tasks and the initiative to lead teams to get the desired results. Currently, holding a Top-Secret Clearance. (TS-SCI)

WORK EXPERIENCE

Cyber Operations Watch Officer

Defense Information Systems Agency, Joint Service Provider, Washington, D.C. – May 2019 - Present
Responsible for network oversight, incident management, incident reporting of critical networks, links, and services for the National Capital Region (NCR) supporting the National Military Command Center (NMCC), Joint Chiefs of Staff (JCS), Office of the Secretary of Defense (OSD) and HQDA. Directly supporting over 45,000 customers across 80 remote locations. Served as the interface between JSP, technicians and the customers providing 24/7 Information Technology (IT)services. Also, responsible for the implementing activity cycle training plans, and shift operational reports.

- Critical role in network design, technical review and implementation for new network infrastructure hardware and network operating systems for voice and data communication networks.
- Decreased the number of critical incidents by 30% by persistently collaborating joint efforts between the customers, vendors, and outside agencies.
- Detected, identified, contained and remediated multiple information security and cybersecurity incidents, trained users and technicians in response procedures.
- Managed 1450 critical incidents for the National Capital Region (NCR) by prioritized resources ensuring a 99.9% "UP" rating to operations and users to ensure minimal downtime and continued Command and Control (C2) support.

Systems Control Officer

Defense Information Systems Agency, Joint Service Provider, Washington, D.C. - August 2018 – May 2019

Responsible for oversight of infrastructure operations of the Technical Control Facility (TCF), which consisted of facilitating worldwide Command, Control, Communications and Intelligence (C3I) services to National Command Authorities, Service Secretaries/Service Chiefs, Combatant Commanders, and other Governmental Agencies across the Defense Information Systems Network (DISN). Responsible for providing 24/7 operations, troubleshooting, and restoration of Metropolitan Area Network (MAN) and DISN circuits that traverse the National Capital Region (NCR), as well as, tracking new projects and Life Cycle Replacement (LCR) projects from planning thru implementation and documentation in support of JSP's strategic missions.

- Restored full operational capabilities to C3I systems by troubleshooting and correcting over 150 system faults.
- Advised the executive leadership on initiatives to improve processes and procedures of daily operations.
- Facilitated the Central Area of Business (CAB) operations for the Pentagon Primary Technical Control Facility (PPTCF) supervising 33 personnel.
- Integrated personnel into High Assurance IP Encryption (HAIPE) Team, increased NCR rekey capability by 50%.
- Conducted daily operation, Quality Assurance/Quality Control (QA/QC), and training with network elements such as Cisco systems, Juniper systems, Nokia Systems, Ciena systems, Larscom, Promina, cryptographic equipment and several other networking hardware devices and systems.

Technical Control Facility Manager
United States Army Network Enterprise Center - Walker, Camp Walker, KR - August 2017- August 2018

Responsible for coordinating and supervising the maintenance and restoration of communication system outages, and ensuring such systems perform at maximum capabilities. Directly responsible for the installation of new equipment, upgrades, and modifications to the existing equipment in the system. Managed Campus and Stations interconnections over SONET, ATM, and DMU Transport Carrier Systems. Managed the operation and maintenance for HVAC, UPS, generator, battery support systems. Directly responsible for the health and welfare of 22 employees and accountability for equipment worth in excess of $3.5 million.

- Monitored and maintained over 1200 circuits that provided secure communication for multiple military units within South Korea, Japan, and various other locations across the globe.
- Hand selected to assist the Network Switching Division in Network Modification (NETMOD), installed 76 switches to upgrade the Area IV network in the lower two thirds of the Korean Peninsula.
- Coordinated and managed the installation of 56 exercise circuits for Ulichi Freedom Guardian (UFG) FY'17 and Key Resolve (KR) FY'18 with 100% availability rate.
- Consistently assumed role as subject matter expert and trainer for office personnel, provided instructions on training shortfalls to increase over efficiency of operations.
- Initiated and took action to correct 15 deficiencies identified during a Force Protection assessment for the facility.
- Developed and revised site certification program and trained team on circuit flow, power maintenance, and diagnostic systems, while maintaining over 1245 data circuits.
- Directly responsible timely calibration of 101 lines of equipment between 4 locations, efforts resulted in a calibration rating of 96.4%

Technical Control Facility Engineer
United States Army, 114TH Signal Battalion, Frederick, MD - October 2014 – July 2017

Responsible for providing joint communications support and restoral of telecommunication circuits, trunk groups, systems and services for the National Command Authority, National Military Command Center, and RRMC.

- Ensured over $56,000,000 of communication equipment was operational in support of the Joint Staff, Office of the Secretary of Defense (OSD), Department of Defense (DoD), Federal Emergency Management Agency (FEMA), and other federal agencies.
- Supervised configuration, operation, and fault isolation of technical control equipment, and associated devices.
- Led restoral actions of more than 250 outages of critical telecommunications services with over 150 of the actions directly supporting the OSD and the Pentagon.
- Directly responsible for maintaining 940 communication circuits at 99.8 percent reliability and 95 percent of all outage were restored prior to reporting requirements.
- Provided communications support for National Level Exercise (NLE) in support of Pentagon, OSD, CJCS, and MEDCOM objectives, while maintaining 99.999% uptime for seamless services during 72hr period.
- Created an environment which encouraged technical proficiency and expertise, which resulted in the Tech Control Facility winning Army Tier III Facility of the Year.
- Attention to detail during monthly maintenance and inventory resulted in 100 percent accountability of task essential communication equipment totaling over $30,000,000.

TECHNICAL SKILLS

- Operating Systems: Windows Server 2008, 2008 R2, 2012 R2, 2016 | Windows 7, Windows 8, Windows 10 | CentOS, Ubuntu, Kali Linux, Parrot OS, macOS
- Network Equipment: Cisco Routers 2600, 2900 Series | Cisco Switches 2900, 3500, 3700 Series |
- Storage and Backup Solutions: Dell EqualLogics | NetApp Fabric Series and Disk Shelves | QNAP Network Attached Storage
- Remote Utilities: VNC | TightVNC | Remote Desktop Services | SSH | Telnet | PuTTy
- Others: WinSCP | SecureCRT | Microsoft Active Directory | PowerShell | NetFlow | SolarWinds Engineer's Toolset | Microsoft Deployment Toolkit (MDT) Windows 10 1607, 1703, 1709, 1803, 1809 | System Center Configuration Manager 2012 R2, System Center 2016
- Tools: Nmap | Metasploit | Cobalt Strike| Burp Suite | Hashcat | JohnTheRipper | Nikto | Nessus
- Languages: Python | JavaScript | HTML | CSS | React

CERTIFICATIONS

- A+ (Issued: June 2017)
- Network+ (Issued: February 2019)
- Security+ (Issued: October 2014)
- Cloud Essentials (Issued: March 2020)
- Project+ (Issued: December 2019)
- Cybersecurity Analyst (CySA+) (Issued: June 2019)
- CompTIA Advanced Security Practitioner (CASP+) (Issued: November 2019)
- Cisco Certified Networking Associate Routing and Switching (CCNA) (Issued: December 2019)
- Certified Information Security Manager (CISM)
- Project Management Professional (PMP) (Issued: January 2021)
- Microsoft Certified Professional (MCP) (Issued: September 2017)
- Certified Ethical Hacker (CEH) (Issued: March 2019)
- Certified Network Defense Architect (CNDA)
- LPI Linux Essentials (Issued: June 2019)
- Site Development Associate (Issued: DEC 2019)
- ITIL Foundations (Issued: May 2019)
- Certified Information Systems Security Professional (CISSP)

EDUCATION

Bachelor of Science, Network Operations and Security | March 2021

Western Governors University, Salt Lake City, UT

Associate of Arts; Psychology | May 2016

Frederick Community College, Frederick MD