

RANDALL ROWLAND

✉ joboffers@randyrowland.me ☎ (478) 287-9987 📧 in/randall-rowland-jr 🌐 https://randyrowland.me

SUMMARY

Seasoned Security Engineer with over 19 years of experience in the United States Air Force, excelling in project oversight, staff leadership, and resource management within dynamic environments. Demonstrates expertise in IT systems, data analysis and risk assessments, and strategic security planning and system design. Possesses an **active Top Secret clearance**. Leveraging Skill Bridge to pivot towards a cybersecurity-focused career, fueled by a passion for continuous learning, with certifications attained through hands-on home lab exploration and dedicated training platforms.

EXPERIENCE

Security Engineer | United States Air Force | Tucson, AZ | November 2018 - Present

- Oversaw Green Belt initiative to optimize Change in the Production Scheduling process, reducing processing time by 66% to 8.2 hours & eliminating duplicate documentation, fortifying organizational resilience against operational disruptions & aligning with stringent security controls & protocols.
- Executed Incident Response (IR) checklist to contain major incidents to protect national security & confidentiality of classified data.
- Architected 9 SharePoint sites, enabling seamless collaboration for 94 users with 12K+ documents, and fortified data security through Identity Access Management (IAM) and Role-Based Access Controls (RBAC), granting precise access to 700+ employees.
- Devised 21 Power Automate tasks, streamlining approvals and reminders to eradicate potential errors and maintain data integrity for 80+ employees.
- Secured a crucial \$40.7K satellite contract, successfully revitalizing secure communications and amplifying aircraft capabilities throughout the Middle East region.
- Maintained and repaired 21 Solaris, Red Hat Enterprise Linux (RHEL), and Windows systems, 3 Cisco network switches, and 2 mil-spec data links for 14 EC-130H Compass Call electronic warfare aircraft valued at \$165 million each, thriving in a fast-paced and high-pressure operational setting.
- Managed 153 personnel's security clearances, ensuring employees maintained eligibility to access classified information.
- Provided and tracked the organization's SETA (Security Education, Training, and Awareness) program to educate employees on security protocols.

Operations Manager | United States Air Force | South Korea | August 2017 - August 2018

- Engineered a streamlined SharePoint workflow, automating sensitive flying operations requests across 4 departments for enhanced efficiency and accuracy.
- Coordinated the synchronization of a \$171 million flying program with the South Korean Air Force by directly overseeing 14 employees, ensuring seamless collaboration and operational alignment.
- Upheld US data confidentiality standards, including NIST Special Publication 800-53, by meticulously implementing classification and control markings, policies, and procedures, safeguarding sensitive information integrity.

Principal Network & Computer Systems Administrator | United States Air Force | Warner Robins, GA | January 2006 - July 2017

- Formulated policies, standards, and procedures guiding an OpenVMS to RHEL migration, ensuring seamless transition and uninterrupted multi-user computer system functionality. Incorporated Linux command references into the organization's standard operating procedures for enhanced usability and efficiency.
- Detected a closed port within a firewall; adeptly reconfigured settings across 3 firewalls to restore crucial communication between airborne and ground IT systems, ensuring operational continuity and system reliability.
- Supervised 6 junior admins, uncovering and rectifying a debilitating database error that hindered system loading; coordinated error resolution, database optimization, and rapid system restoration for improved performance. Spearheaded training sessions for 20 junior admins, imparting knowledge in emerging computer systems and software, thereby enhancing aircraft capabilities and operational effectiveness.
- Conducted performance evaluations for 57 admins, promptly identifying and addressing human performance gaps, and delivering constructive feedback to facilitate personnel development and growth. Conducted audits of junior admins' computer and network operations to ensure compliance with Security Technical Implementation Guides (STIGs) and organizational policies, maintaining

security and operational integrity.

EDUCATION

MS, Cybersecurity | SOUTHERN NEW HAMPSHIRE UNIVERSITY | Minor in IT Management | Manchester, NH | 2024 | 3.810

BS, Cybersecurity | SOUTHERN NEW HAMPSHIRE UNIVERSITY | Minor in Secure Programming | Manchester, NH | 2022 | 3.6

BS, Computer Science | AMERICAN SENTINEL UNIVERSITY | Minor in Game Programming | Aurora, CO | 2017

AAS, Information Systems Technology | COMMUNITY COLLEGE OF THE AIR FORCE | Montgomery, AL | 2014

CERTIFICATIONS

Continuous Process Improvement Green Belt | USAF Continuous Improvement & Innovation | 2024

Cybersecurity Analyst+ (CySA+) | CompTIA | 2023

Certified Information Systems Security Professional (CISSP) | ISC2 | 2021

Security+ | CompTIA | 2020

Server+ | CompTIA | 2020

Network Infrastructure Professional | CompTIA | 2020

Certified Linux Administrator (LPIC-1) | Linux Professional Institute (LPI) | 2019

Linux+ | CompTIA | 2019

Linux Network Professional | CompTIA | 2019

Network+ | CompTIA | 2019

INVOLVEMENT

Incident Response Foundations Course Moderator | Deadwood, SD | Wild West Hackin' Fest | October 2023

- Facilitated a comprehensive 16-hour Incident Response Foundations course for 30 students under the instruction of Derek Banks. Provided valuable support to both the instructor and students during Back Doors & Breaches Incident Response Tabletop Exercises. Distributed Incident Response handbooks featuring example IR Policy and Procedure documentation to enhance learning outcomes.
 - Acquired proficiency in fundamental concepts of Incident Response, including the essentials of successful IR programs and teams, critical components of IR policies and procedures, network traffic monitoring techniques, endpoint logging requirements, and strategies for addressing logging failures. Deepened understanding of key Active Directory event IDs for detecting and mitigating attacker activity, and considerations for incident response in cloud environments. Assisted students in applying these concepts to practical scenarios.
 - Managed the setup and operation of AV equipment and computer systems to facilitate seamless connectivity for 10 virtual students participating in the instructional session.
-

SKILLS

Process Improvement | Stakeholder Engagement | Project Management | Program Management | Organizational Leadership | Personnel Management | Operations Management | Team Development & Leadership | Training & Development | System Design | System Integration | Information Assurance | Information Security | Physical Security | TEMPEST | Kanban | IT Systems | Network Protocols | Markdown | BASH Scripting | NIST SP 800-53B, 800-171, 800-175A | NIST CSF | CIS Benchmarks | STIGs | VLANs | VPNs: OpenVPN, Wireguard, IPsec | Microsoft Office | SharePoint | Jira | BMC Remedy | Git | Git Kraken | SolarWinds | Windows | Linux: Red Hat Enterprise Linux, Ubuntu, Fedora | OpenVMS | Solaris | TrueNAS | pfSense firewall: HA-Proxy, ACME LetsEncrypt Certificates, ntopng | Proxmox | Containerization: Docker, LXC | SolarWinds | Wireshark | MISP | Joplin | Notion | Snipe-IT | Kasm Workspaces | Nextcloud | UniFi | NetBox | SIEMs: Security Onion, Elasticsearch, Wazuh | IDS/IPS: Zeek, Suricata, AC-Hunter, CrowdSec