Nicholas A. Southern

Greater Orlando, FL | southerncybersolutions@protonmail.com | linkedin.com/in/nicholas-southern

Targeting: Security Operations Center (SOC) Analyst | **Clearance:** Active TS/SCI

PROFESSIONAL SUMMARY

Operational Cybersecurity Analyst with 6+ years of experience in 24/7 Network Operations Centers (NOC), Incident Response, and classified DoD environments. Proven expertise in SIEM tuning (Splunk), Endpoint Detection & Response (EDR), and AI-driven threat analysis. Skilled in translating "compliance noise" into actionable defense signals using NIST 800-171 and 800-53 frameworks. Fully prepared for rotational shift work, leveraging a background in high-tempo USAF mission support to maintain continuous security monitoring.

TECHNICAL & OPERATIONAL COMPETENCIES

SOC Operations | Incident Triage, Threat Hunting, Log Analysis, Root Cause Analysis, 24/7 Watch Floor Ops
Security Tools | Splunk (SIEM), McAfee HBSS (EDR), ACAS, Drata, Remedy / WebHelpDesk
AI Security | LLM Red Teaming, Prompt Injection Defense, Adversarial Machine Learning, RLHF
Compliance | NIST 800-171 (University/Research Std), NIST 800-53, HIPAA / FERPA Awareness
Systems / Scripting | Red Hat Enterprise Linux (RHEL), Bash Scripting, Windows Server, Azure

PROFESSIONAL EXPERIENCE

AI Cybersecurity Specialist (Contract) — Invisible Technologies — Remote
Dec 2025 – Present

- Analyze emerging AI-driven attack vectors, specifically focusing on prompt injection and adversarial manipulation of Large Language Models (LLMs).
- Conduct "Red Team" scenarios to identify vulnerabilities in AI model responses, tuning safety guidelines to prevent data leakage and harmful outputs.
- Provide technical feedback on code generation and security exploits, enhancing the robustness of AI-assisted threat analysis tools.

Senior Multi-Functional Information Security Analyst — Lockheed Martin — Jacksonville, FL
June 2024 – Jan 2026

- Engineered Splunk dashboards for real-time security event analysis, tuning correlation rules to reduce false positives and ensure 100% audit log retention.
- Enforced NIST 800-171 compliance standards across RHEL and Windows environments, directly supporting data security requirements similar to higher-education research frameworks.
- Executed technical vulnerability assessments and STIG hardening, serving as the primary incident handler for system deviations and security alerts.
- Mentored junior staff on RMF packages and standard operating procedures (SOPs), fostering a culture of continuous monitoring and rapid response.

Information Assurance Analyst (Contract) — Five Stones Research Corporation — Jacksonville, FL
Sep 2023 – Nov 2023

- Configured McAfee HBSS (Host Based Security System) for Endpoint Detection & Response (EDR), ensuring continuous visibility into threat activity on classified networks.
- Conducted forensic analysis of endpoint logs to identify indicators of compromise (IOCs) and validate system integrity.
- Managed incident response workflows for system outages and security breaches, ensuring strict adherence to DoD incident reporting timelines.

Network Operations Center Engineer & Systems Administrator — United States Air Force — Ramstein AB, Germany
Apr 2019 – Jan 2023

- Managed 24/7/365 network defense operations for 3,000+ personnel; highly experienced with rotational shifts, nights, weekends, and holiday schedules.
- Resolved 1,000+ Tier 1 / Tier 2 incidents for JWICS / ISR networks, performing rapid triage and containment of critical connectivity and security issues.

- Mitigated zero-day vulnerabilities across 241 systems within 24 hours, preserving system accreditation during high-threat windows.
- Administered Red Hat Enterprise Linux servers, maintaining 99.9% uptime through rigorous patch management and proactive log monitoring.

EDUCATION & CERTIFICATIONS

B.S., Cyber Security & Information Assurance — Western Governors University Salt Lake City, UT
Expected Dec 2026

GIAC | Security Essentials (GSEC), Foundational Cybersecurity Technologies (GFACT)
CompTIA | Security+ CE (DoD 8570 Compliant), Network+ (N10-009), A+
Service Mgmt | ITIL 4 Foundation