ALEK NORRIS

319-327-2111 | Alek.P.Norris@outlook.com |Ankeny, IA | Secret

CYBERSECURITY ENGINEER | IT PROFESSIONAL

Veteran and cybersecurity professional with 8 years' experience spanning military SATCOM/IT, cloud engineering at Microsoft, and a B.S. in Cybersecurity Engineering. I bring 3+ years in IT and a security-focused mindset that goes beyond simply identifying what happened, I dig into how and why incidents occur, drawing on a deep, low-level understanding of operating systems and security mechanisms. I've worked across endpoints, cloud, SaaS, and identity platforms to fully grasp the context and impact of emerging threats. My curiosity and drive to learn help me get to the root of complex issues and communicate findings clearly to both technical teams and leadership. Currently seeking to apply a security-focused, automation-driven mindset to detect, defend, and respond to evolving cyber threats across modern environments.

KEY SKILLS

- **Security Operations** | SIEM, IDS/IPS, Splunk, Snort
- **Vulnerability Mgmt** | Nessus, patch orchestration
- **Languages** | Python, Bash, PowerShell, C, Java, JavaScript
- **Network Security** | VPNs, SDN, firewalls, iptables
- **Identity & Access** | Azure AD, SSO, RBAC, Zero-Trust
- **Cloud & SaaS Security** | Windows Server, Azure, IAM logging
- **Endpoint & EDR** | AV/EDR, DLP, disk encryption, host hardening
- **Threat Hunting & Forensics** | MITRE ATT&CK, Autopsy, Ghidra
- **Incident Response** | Root-cause, Log analysis, containment
- **Documentation & Support** | SOPs, briefs, user training

PROFESSIONAL EXPERIENCE

Iowa State | HEBSE Database | Cybersecurity Engineer

August 2024 - May 2025

- **LLM-Driven NLP Interface:** Integrated a transformer-based AI service that translates plain-English questions into parameterized SQL, letting non-technical users query terabytes of HEBSE data securely and slashing analyst support time by 70 %.
- **Secure Web App & Host Hardening:** Engineered a React/Python–PostgreSQL platform; hardened Linux & Windows hosts, enabled granular RBAC, and safeguarded credentials with AES-256, and secure storage an handling of data—shrinking attack surface.
- **Automated Container Patching:** Scripted image updates and dependency scans, slashing manual patching effort by 50% and generating detailed logs that speed remediation and enhance overall security posture of the app while in development.

Microsoft | MSSA Cloud Engineer

January 2021 - June 2021

- ***Server & Cloud Administration:*** Completed Microsoft-led training in server and cloud security, focusing on Azure IAM, Active Directory, and secure networking practices.
- ***Virtual Networks & Security:*** Gained hands-on experience with Azure Virtual Networks, DNS hardening, firewall configurations, and role-based access controls (RBAC) to ensure secure infrastructure deployment.

U.S. Army | Satellite Communications Engineer | Classified Asset & Operations Manager

August 2017– July 2021

- ***Tier-1/2 Support & Endpoint Hardening:*** Provided frontline troubleshooting and escalation, managed encryption keys, applied patches, and enforced endpoint-hardening standards.
- ***Network Engineering & Site Infrastructure:*** Configured and maintained Cisco and Brocade routers/switches supporting site-wide tactical communications across a large LAN/WAN hybrid environment. Ensured 99.9% uptime and stable routing under dynamic operational loads.
- ***Routing, Secure Communication & Compliance:*** Designed and optimized network infrastructure for classified DoD environments, configuring DHCP, static routing, VLANs, encrypted VPNs, and integrating firewalls, access controls, and segmentation. Managed firewall configurations and encryption protocols to ensure secure, high-availability communications in compliance with DoD security frameworks and zero-trust principles.

LinkedIn:linkedin.com/in/aleknorris **Git:**Anorris98 **Portfolio:**aleknorris98.wixsite.com/aleknorris

EDUCATION

Bachelor of Science in Cybersecurity Engineering
Iowa State University – 2025

- (EAC) of ABET-accredited cybersecurity engineering program emphasizing practical integration of computer engineering and science, secure systems design, and applied cybersecurity through extensive labs, research projects, and collaborative development.
- ***Key Coursework:*** Cryptography; Information Warfare & Attack-Vector Analysis; Penetration Testing; Network & Wireless Security; Network Protocols & Graph Theory (DSA applications); TCP/IP & Linux; Digital Forensics; Systems Auditing & Risk Assessment (IEEE/NIST); Embedded Systems Programming; Python, C, Java, Assembly.

CERTIFICATIONS

Security+ (04/2028)**, Network+** (04/2028)**, IT Fundamentals**

SELECTED ACCOMPLISHMENTS

Cybersecurity & Incident Response

- ***Vulnerability Assessment & Penetration Testing:*** Performed penetration testing and vulnerability assessments utilizing Nessus, Nmap, Wireshark, and Metasploit to identify, document, and mitigate security vulnerabilities.
- ***Network Security & Threat Detection:*** Investigated live network traffic anomalies, identifying lateral movement and adversarial TTPs using MITRE ATT&CK methodologies. Conducted forensic analysis and malware reverse engineering using Ghidra to detect and mitigate new threats.
- ***Information Warfare & Incident Response*:** Participated in forensic investigations of security breaches, log correlation analysis, and SIEM-based threat monitoring, applying real-time security controls to neutralize attack vectors.
- ***Cryptography & Secure Systems:*** Implemented modern cryptographic algorithms (AES, RC4, DES, PKI) in Python for secure data transmission, digital signatures, and encrypted communication protocols. Explored homomorphic encryption for secure data processing.

Secure Software Engineering & Development

- ***Custom Multi-Threaded Program:*** Built a multi-threaded application implementing secure memory management, synchronization techniques (mutex, signaling variables), and robust memory handling, demonstrating capability in secure software development.
- ***POSYDON Project (Full-Stack & Security):*** Developed a React/Python web app backed by PostgreSQL for querying multi-TB datasets via generative AI; secured all communications with PKI-authenticated SSH tunnels and HTTPS; and deployed a file-based binary-hosted AES-256-GCM service to encrypt data at rest and in motion.

Embedded Systems & Hardware Security

- ***Multistage MIPS Processor:*** Designed and tested a multi-stage MIPS processor in VHDL with hardware-based forwarding, hazard detection, and assembly validation.
- ***CyBot Embedded Systems Project:*** Engineered an embedded navigation and scanning system, developing secure embedded software in C with UART communications, enabling wireless area scanning and remote operation.

Independent Research Project – DNS Tunneling & Traffic Analysis

- Built a multi-VM dnsmasq + dnscat2 testbed in a VPN-gated, firewalled environment, then extended it to a real-world deployment. Registered a public domain via Google and tunneled covert communications from the isolated network to an EC2-hosted DNS server (NS1). Captured and analyzed DNS query/response traffic to characterize tunneling behavior and develop detection heuristics.