Abdulaziz Alghamdi

Cybersecurity Engineer

📱* +1 (720) 400-1869
✉ [regular] azizcsecj@gmail.com
🌐 aziz707.info
in aziz-alghamdi-525810360
☐ azizalghamdi

Professional Summary

Bilingual Cybersecurity Engineer with comprehensive expertise in security architecture, threat detection, and incident response. Native Arabic and English speaker with proven track record of implementing robust security monitoring systems, reducing phishing vulnerabilities by 75%, and developing automated security solutions. Combines strong technical foundation in multiple programming languages with specialized cybersecurity knowledge and criminal justice insights. Seeking to leverage hands-on experience with enterprise security tools and DevSecOps practices to strengthen organizational security posture in the Gulf region's rapidly evolving digital transformation landscape.

Education

2021–2025	**Bachelor of Arts & Science in Computer Science**, *University of Colorado at Colorado Springs*, Colorado Springs, CO **Cybersecurity Track** with Minor in Criminal Justice **Relevant Coursework:** Network Security, Cryptography, Digital Forensics, Secure Software Development, Risk Management, Incident Response **Activities:** National Cyber League Competitor, Mountain Lions Cyber Club Member

Core Technical Skills

Security Engineering	SIEM Implementation & Management • Vulnerability Assessment & Penetration Testing • Incident Response & Digital Forensics • Security Architecture Design • Risk Assessment & Management • Compliance & Audit (NIST, ISO 27001)
Security Tools	Splunk • QRadar • Wireshark • Metasploit • Nmap • Burp Suite • OWASP ZAP • Nessus • OpenVAS • Tripwire • Snort • pfSense • CrowdStrike • SentinelOne
Programming & Automation	Python (Security Automation, Scripting) • C/C++ • Java • JavaScript • SQL • PowerShell • Bash • Go • Rust • PHP
Platforms & Infrastructure	Linux (Ubuntu, CentOS, Kali) • Windows Server • AWS • Azure • Docker • Kubernetes • VMware • Active Directory • TCP/IP Networking
Security Frameworks	NIST Cybersecurity Framework • OWASP Top 10 • CIS Controls • MITRE ATT&CK • SANS Top 25 • ISO 27001/27002 • SOC 2 • Saudi CITC Cybersecurity Framework • UAE Cybersecurity Council Guidelines

Security Engineering Experience & Projects

2024–2025	**Security Operations & Monitoring**, *Academic & Personal Projects* • **SIEM Implementation:** Deployed and configured Splunk environment, created 20+ custom detection rules, reducing false positives by 60% • **Incident Response:** Developed comprehensive IR playbooks and conducted tabletop exercises, improving response time by 40% • **Vulnerability Management:** Implemented automated scanning workflows using Nessus and OpenVAS, identifying and remediating 95% of critical vulnerabilities
2023–2024	**Security Automation & DevSecOps**, *Personal Development Projects* • **Python Security Tools:** Built custom security automation scripts for log analysis, threat hunting, and compliance reporting • **Infrastructure Security:** Designed secure cloud architectures on AWS with proper IAM, encryption, and monitoring configurations • **CI/CD Security:** Integrated security testing into development pipelines using SAST/DAST tools and container scanning
2023–2024	**Network Security & Penetration Testing**, *Academic Projects* • **Network Defense:** Configured firewalls, IDS/IPS systems, and network segmentation reducing attack surface by 70% • **Penetration Testing:** Conducted authorized security assessments using Metasploit, Burp Suite, and custom tools • **Security Awareness:** Led cybersecurity training program resulting in 75% reduction in successful phishing attempts

Certifications & Professional Development

2025	**Google Cybersecurity Professional Certificate** - Security Operations, Incident Response, Python Automation
In Progress	**CompTIA Security+** (Scheduled: June 2025) • **Certified Ethical Hacker (CEH)** (Scheduled: August 2025)
2024	**AWS Cloud Practitioner** • **Linux Professional Institute Certification (LPIC-1)** • **Python Institute PCAP**

Key Achievements & Recognition

- **Security Impact:** Reduced organizational phishing susceptibility by 75% through comprehensive security awareness program
- **Automation Success:** Developed ML-based anomaly detection system achieving 92% accuracy in threat identification
- **Competition Performance:** Top 25% finisher in National Cyber League individual competition (Fall 2024)
- **Technical Leadership:** Led 5-person cybersecurity capstone project implementing enterprise-grade security monitoring solution

Additional Competencies

Leadership — Project Management • Cross-Cultural Team Leadership • Technical Documentation • Security Awareness Training • Stakeholder Communication • Risk Communication to C-Level Executives

Languages — Arabic (Native) • English (Native-level since age 16) • Spanish (Conversational)

Global Experience — Bilingual Technical Communication • Cross-Cultural Cybersecurity Implementation • Gulf Region Technology Landscape Understanding