ABDULAZIZ ALSIDRANI

Cybersecurity Analyst | Blue Team & SOC Operations | Detection Engineering | CompTIA Security+
+966 552716717 | az.alsidrani@gmail.com | linkedin.com/in/az-alsidrani | izltx.github.io | Riyadh, Saudi Arabia

PROFESSIONAL SUMMARY

Certified Cybersecurity Analyst (CompTIA Security+) specializing in Blue Team operations, Detection Engineering, and SOC automation. Engineered an AI-powered alert triage pipeline integrating Splunk SIEM with a locally-hosted LLM, reducing triage time to ~30 seconds with 94% AI confidence across 5 MITRE ATT&CK techniques. Built Python-based threat intelligence tooling cutting manual IOC triage by 80%. Seeking a SOC Analyst or Detection Engineering role to deliver immediate value in log analysis, alert triage, and incident response.

TECHNICAL SKILLS

SIEM & Detection: Splunk (SPL), Custom Alert Rules, Event Correlation, Windows Event Logs, Security Monitoring
SOC Operations: Alert Triage, Threat Hunting, Incident Response, MITRE ATT&CK Mapping, Log Analysis
Telemetry & Endpoint: Sysmon, Windows Event Forwarding (WEF), Active Directory Security, Endpoint Hardening
Automation & TI: Python, LLM Integration (Ollama), VirusTotal API, Shodan API, IOC Analysis, OSINT
Infrastructure: Proxmox VE, pfSense, Apache Guacamole, Windows Server, Linux, Network Traffic Analysis

PROJECTS

AI-Powered SOC Triage Engine & Enterprise Detection Lab — Mar 2026 – Present

- Architected a virtualized enterprise SOC on Proxmox VE with Active Directory, Sysmon telemetry, and Splunk SIEM integration for centralized log aggregation and security monitoring across all endpoints.
- Engineered a fully automated AI alert triage pipeline (Splunk + Ollama LLM) reducing triage time to ~30 seconds per alert with 94% classification confidence, eliminating manual first-response bottlenecks.
- Developed custom SPL detection rules mapped to MITRE ATT&CK: Brute Force (T1110) via Event ID 4625 and Privilege Escalation (T1098) via Event IDs 4720/4728; routed results to Discord and Splunk HEC.

Automated Threat Intelligence & IOC Triage Tool — Oct 2025 – Jan 2026

- Built a Python-based IOC aggregator integrating VirusTotal and Shodan APIs, reducing manual triage time by 80% with input sanitization to prevent payload execution and secure API key management.

Graduation Project: Isolated Cybersecurity Lab Platform (Proxmox) — Jan 2026 – Apr 2026

- Architected a multi-tenant virtualized lab on Proxmox VE with pfSense network isolation, Apache Guacamole clientless access, dual-role access control, and CTFd for live Incident Response and log analysis scenarios.

PROFESSIONAL EXPERIENCE

Cybersecurity Intern — CS & Engineering Department — Jun 2025 – Aug 2025

King Fahad Medical City (KFMC) · Riyadh, Saudi Arabia

- Conducted security audits on backend data flows, implementing input validation and sanitization controls to mitigate SQL/NoSQL injection vulnerabilities across critical healthcare systems.
- Enforced application security logging baselines, enhancing auditability and security monitoring visibility across regulated healthcare infrastructure.

EDUCATION

Bachelor's Degree, Cybersecurity — Aug 2021 – Jun 2026

University of Hafr AlBatin · Saudi Arabia

CERTIFICATIONS & MEMBERSHIPS

CompTIA Security+ ce — CompTIA — Feb 2026 – Feb 2029
IBM SkillsBuild Cybersecurity Professional Certificate — IBM — Jun 2025
Student Member Engineer — Saudi Council of Engineers (SCE)

LANGUAGES

Arabic: Native | **English:** Professional Working Proficiency