

Abdullah Albannay

Phone: +966-55-123-4567 | Email: abdullah.albannay.demo@example.com | LinkedIn: [linkedin.com/in/abdullah-albannay-demo](https://www.linkedin.com/in/abdullah-albannay-demo)

Professional Summary

Cybersecurity Expert with 9+ years of hands-on experience in offensive and defensive security, threat hunting, incident response, and cloud security. Proven track record designing secure architectures, conducting red-team/blue-team exercises, and hardening enterprise systems. Strong communicator who translates technical risk into business decisions and leads cross-functional teams to improve security posture.

Core Competencies

- Threat Hunting & Incident Response
- Red Teaming & Penetration Testing (web, network, cloud)
- Secure Architecture & Cloud Security (AWS, Azure)
- Vulnerability Management & Secure SDLC
- SIEM / EDR Tuning & Forensics
- Scripting & Automation (Python, Bash, PowerShell)
- Identity & Access Management (IAM)
- Security Policy, Risk Management & Compliance (ISO 27001, NIST)

Professional Experience

Senior Cybersecurity Engineer — SecureWave Solutions (Riyadh, KSA)

Apr 2020 - Present

- Lead incident response and threat-hunting operations across 24/7 environments, reducing mean time to containment by 45%.
- Designed and implemented cloud security baselines for AWS and Azure (CSPM, IAM hardening, network segmentation), cutting misconfigurations by 60%.
- Conducted quarterly red-team engagements and purple-team exercises; produced remediation roadmaps and tracked remediation through to closure.
- Developed automation playbooks (Python/PowerShell) to triage alerts and enrich IOC data into the SIEM.

Cybersecurity Analyst — GulfTech Cyber (Jeddah, KSA)

Jul 2016 - Mar 2020

- Performed vulnerability assessments and penetration tests for web applications and internal networks; authored concise executive and technical reports.
- Implemented SIEM correlation rules and EDR policies to reduce false positives and improve detection of lateral movement.
- Led security awareness workshops and tabletop exercises for senior stakeholders.

Education

M.Sc. in Cybersecurity — King Saud University (Riyadh, KSA), 2016

B.Sc. in Computer Science — King Abdulaziz University (Jeddah, KSA), 2013

Certifications

- CISSP — (ISC)² (2021)
- Offensive Security Certified Professional (OSCP) — Offensive Security (2018)
- Certified Cloud Security Professional (CCSP) — (ISC)² (2022)
- AWS Certified Security – Specialty (2023)

Selected Projects

- Enterprise Cloud Hardening — Led a cross-functional program to implement IaC security checks and automated remediation across AWS accounts; reduced drift and improved compliance posture.
- Purple Team Program — Built recurring purple-team exercises aligned to MITRE ATT&CK to validate detection and response coverage.
- Automated Threat-Enrichment Pipeline — Created a pipeline that ingests alerts, enriches with threat intel, and files actionable incidents for analysts.

