Mohammed Aldahash *Cyber Security Consultant*

MohammedAldahash@outlook.com | 0533060221 | Riyadh | Linkedin.com/in/MohammedAldahash

Cybersecurity Consultant with 4+ years of experience in SOC operations, administration, and incident response. Certified and passionate about understanding environments to implement proper protection, detection, and response.

PROFESSIONAL EXPERIENCE

Elm

Cyber Security Consultant 2026 – Present | Riyadh, Saudi Arabia

- Lead the SOC Enablement unit to ensure comprehensive security visibility over 10K+ assets and 23 NCA-critical applications across hybrid multi-cloud and containerized environments for multiple subsidiaries.
- Oversee the full lifecycle (design, deployment, and operations) of SIEM, XDR, CNAPP, DLP, and M365 E5 platforms.
- Automate visibility KPI reporting for asset coverage and required log types against the organization's CMDB as per the organization's log standard.
- Serve as the primary technical point of contact for the SOC, aligning operations with the strategic objectives of GRC, Security Architecture, Internal Audit, and ERM teams.

Cyber Security Senior Analyst 01/2025 – 12/2025 | Riyadh, Saudi Arabia

- Investigated L1-escalated alerts; contained and documented incidents end-to-end.
- Built use cases to close MITRE ATT&CK coverage gaps mapped to the organization's threat model.
- Created procedures, KPIs, dashboards, reports, shift schedules, and playbooks for SOC
- Worked closely with SIEM Admins and IT teams to close visibility gaps in SIEM and raise infrastructure risks to GRC.

Ministry of Education

Cyber Security Specialist (SOC Engineer) 01/2024 – 12/2024 | Riyadh, Saudi Arabia

- Administered SIEM/SOAR/NDR solutions.
- Enhance security detection by creating and testing use cases that cover gaps in the organization's MITRE TTPs.
- Configured and onboarded logs from endpoints, security solutions, and network devices to SIEM.
- Conducted PoCs to test security solutions and create evaluation reports.

Cyber Security Analyst (L1) 06/2022 – 12/2023 | Riyadh, Saudi Arabia

- Triaged alerts on SIEM from EDR, IPS, IDS, WAF, FW, and escalated true positives in a 24x7 SOC.
- Documented all analysis of alerts and incidents on a SOAR following approved playbooks
- Responded to incidents and IOCs from NCA's Haseen portal and contacted relevant teams for any necessary further actions.

EDUCATION

Bachelor's degree, Information Technology (Cybersecurity Track), 08/2017 – 08/2022
Al Majmaah University (4.3 cGPA) Al Majmaah, Saudi Arabia
Graduation project focused on improving website availability by utilizing AWS cloud services

CERTIFICATES

GIAC Defensible Security Architect (GDSA)
(WIP)

GIAC Cloud Forensics Responder (GCFR)
(1/2026)

GIAC Continuous Monitoring Certification (GMON)
(4/2025)

GIAC Certified Detection Analyst (GCDA)
(4/2024)

OffSec Defense Analyst (OSDA)
(12/2023)

eJPTv2
(8/2023)

CompTIA Security+ & CySA+
(1/2023)

AWS Certified Cloud Practitioner
(12/2021)

SKILLS

Log Analysis (QRadar/Elastic/Sentinel/Defender/XSIAM/Splunk/SecOps/) | Cloud (Azure/GCP/AWS/OCI) | Frameworks and controls (NCA, NIST, CIS, and MITRE) | Incident response | Windows/Linux/Kubernetes | Threat Intelligence | Network/Cloud Security | Communication | Leadership