Sari Yaseen Taher

Cybersecurity Consultant

sa-ry@hotmail.com +966597000189 Saudi Arabia Saudi sari-taher Officialsarii

PROFILE

Cybersecurity consultant with over four years of experience delivering and managing incident response engagements across enterprise environments. Regularly leads high severity investigations, coordinates response activities, and supports stakeholders through containment, recovery, and post incident improvement. Brings strong hands on expertise in detection engineering, threat hunting, and digital forensics, with a proven track record of improving SOC maturity through governance, automation, performance metrics, and structured operating models aligned with business risk.

EXPERIENCE - OVER 4Y

2025/12 – Present
Riyadh, Saudi Arabia
CyberSecurity Consultant, *Accenture*

2024/02 – 2025/12
Riyadh, Saudi Arabia
Cybersecurity Trainer, *Tuwaiq Academy*

2025/08 – 2025/12
Riyadh, Saudi Arabia
Cybersecurity Expert, *Tamkeen Technologies*

2024/09 – 2025/08
Riaydh, Saudi Arabia
Digital Forensics and Incident response Consultant, *Tamkeen Technologies*

2022/09 – 2024/09
Riyadh, Saudi Arabia
Senior Cybersecurity Analyst, *Cipher company*

2022/03 – 2022/09
Riyadh, Saudi Arabia
SOC Analyst - Internship, *Cipher company*

EDUCATION

Madinah, Saudi Arabia **B.Sc. Cybersecurity & Digital Forensics,** *Prince Mugrin University*

CERTIFICATES

GIAC Cerified Forensics Analysis — GCFA

Offsec Defense Analysis — OSDA

GRP Professional — GRCP

Malware Analysis Professional — eCMAP

Threat Hunting Professional — eCTHPv2

Digital Forensics Professional — eCDFP

Professional Penetration Tester — eCPPTv2

CORE SKILLS

SOC Leadership & IR
triage frameworks, escalation matrices, major incident command, post-incident reviews, executive comms

Threat Hunting & Detections
hypotheses (CTI-driven & adversary-tool-driven), correlation logic, anomaly baselining, ATT&CK mapping, Sigma/YARA

Adversary Emulation
lateral movement, credential access, persistence, C2 beaconing analytics, living-off-the-land tradecraft

Automation & SOAR
playbooks for isolation, IOC blocking, credential resets, approvals, status broadcasts, evidence kits

Governance
ISO 27001 ISMS practices, SOC process maturity uplift (CMM), KPI programs (MTTD/MTTR, TPR/FPR, SLA)

TECHNICAL SKILLS

SIEM / Analytics
Splunk, ELK, LogRhythm, Exabeam, Wazuh

Email Security & Sandbox
Proofpoint (policy, quarantine triage), VMRay (behavioral detonation and IOC extraction)

Forensics
Volatility, Velociraptor; registry/artifact parsers; timeline tooling and evidence hygiene

Governance
ISO 27001 ISMS concepts; process maturity (CMM) and KPI programs

EDR / NDR
CrowdStrike, Cybereason; ExtraHop (NDR).

SOAR / IR
FortiSOAR playbooks (isolation, IOC blocking, credential resets), approvals, webhooks, evidence packaging

Scripting
C++, Python, Bash, Batch (investigation utilities, automation)

PROJECTS

CMM
Risk-driven CMM achieved for SOC.

ISO 27001

LANGUAGES

- Arabic: Native
- English: Fluent

Sari Yaseen Taher sa-ry@hotmail.com