Ahmad Saud Alassaf

Cybersecurity Professional · Senior Cybersecurity Analyst

Riyadh, Saudi Arabia · +966 50 515 6763 · AhmadSAlassaf@gmail.com · linkedin.com/in/AhmadSAlassaf · alassaf.site

Cybersecurity professional with a Master's degree in Cyber Security and seven years of experience in government and sovereign-fund environments. Combines hands-on offensive security with programme management: planning and delivering penetration-testing and vulnerability-management programmes, designing attack-simulation and phishing exercises, and ensuring alignment with National Cybersecurity Authority requirements and external audit expectations. Experienced in security policy and procedure writing, budgeting for security initiatives, and reporting to executive management.

CORE COMPETENCIES

Security programme management
Planning, scoping, and scheduling of penetration-testing and vulnerability-management programmes; coordination of third-party assessors; remediation tracking and closure metrics.

Governance, risk, and compliance
Alignment with National Cybersecurity Authority controls; audit preparation and evidence management; coordination with internal and external auditors.

Offensive security
Network, web application, and API penetration testing (black, gray, and crystal box); compromise assessment; adversary emulation.

Security awareness and validation
Attack-simulation and phishing campaign design, execution, and measurement of detection, response, and user behaviour.

Policy and procedure development
Drafting and maintaining security policies, standards, and operating procedures aligned with regulatory frameworks.

Executive engagement
Budgeting and business cases for security initiatives; risk-based reporting to leadership; stakeholder and vendor management.

EDUCATION

2026 — **Master in Cyber Security**
Saudi Electronic University, Kingdom of Saudi Arabia

Jan 2017 — **Bachelor of Computer Engineering**
University of Hail, Kingdom of Saudi Arabia

PROFESSIONAL EXPERIENCE

Dec 2020 – Present — **Senior Cybersecurity Analyst — Public Investment Fund**

- Plan and deliver the penetration-testing programme covering networks, web applications, and APIs, including scope definition, scheduling, and coordination of third-party assessors.
- Operate the vulnerability-management programme: asset coverage, risk-based prioritisation, remediation ownership, and closure reporting to management.
- Design and execute attack-simulation and phishing exercises to measure detection, response, and awareness, and translate results into control improvements.
- Support alignment with National Cybersecurity Authority requirements and prepare evidence and responses for internal and external audits.
- Draft security policies and procedures and contribute to budgeting and planning for assessment and tooling initiatives.
- Conduct benchmark compliance checks against hardening baselines and report deviations with remediation guidance.

Feb 2019 – Nov 2020

Senior Information Security Engineer — Ministry of Foreign Affairs

- Conducted network, web application, and API vulnerability assessments and penetration tests using black, gray, and crystal box approaches.
- Led compromise assessments and web application firewall request audits for internet-facing services.
- Reported findings with business impact and prioritised remediation guidance to application owners and management.

CERTIFICATIONS

OSCE — Offensive Security Certified Expert (Nov 2020)

GXPN — GIAC Exploit Researcher and Advanced Penetration Tester (Jun 2020)

GDAT — GIAC Defending Advanced Threats (Feb 2023)

GWAPT — GIAC Web Application Penetration Tester (Jan 2020)

GPEN — GIAC Penetration Tester (Jul 2019)

OSCP — Offensive Security Certified Professional (Dec 2018)

eCPPT — eLearnSecurity Certified Professional Penetration Tester (Aug 2018)

eJPT — eLearnSecurity Junior Penetration Tester (Jan 2018)

EMC Academic Associate — Cloud Infrastructure and Services

INDEPENDENT PROJECTS

Selected

- **TrustedChain** — public threat-intelligence service classifying domains, IPs, and hashes against several hundred thousand curated indicators, with evidence-backed verdicts and an API.
- Self-hosted security-monitoring and hardening programme across cloud and on-premise hosts, with executive reporting and audit-ready evidence.
- Operating model for AI agents with least-privilege credentials, human approval for sensitive actions, and monitoring of agent behaviour.
- Further write-ups, including a bilingual real-estate valuation platform and IoT platforms, are published at alassaf.site/blog.

TECHNICAL SKILLS AND LANGUAGES

Platforms	Linux, Windows, macOS; VMware, VirtualBox; SIEM and file-integrity monitoring
Programming	Python, PHP, JavaScript, SQL
Languages	Arabic (native), English (professional)