Ahmed Alderai

Cyber Security Expert | Senior Security Leader
London · Ahmed@alderai.uk · +44 7584 848 762
LinkedIn: https://www.linkedin.com/in/ahmedadel1991/ · Website: https://alderai.uk
Work Authorisation: UK Partner Visa (no sponsorship required)

PROFESSIONAL SUMMARY

Cybersecurity leader with **13+ years** of experience across financial services, telecommunications, cloud, and other regulated environments. Deep expertise in second-line cyber risk oversight, control framework design, security governance, SOC operations, and regulatory compliance (ISO 27001, NIST CSF, NIS2, PCI-DSS, GDPR). Proven track record translating regulatory expectations and risk appetite into technical controls, delivering board-level risk reporting, and leading cross-functional security initiatives across multi-country operations. Combines senior leadership, stakeholder engagement, and delivery management with genuinely hands-on foundations in penetration testing, SIEM engineering, and cloud security. Currently serving as Principal Information Security Engineer at Lebara Group, leading enterprise and telecom security risk assessments across MVNO operations and eSIM security programmes.

CORE COMPETENCIES

Security Leadership & Governance Security Strategy & Programme Leadership · Second-Line Risk & Control Oversight · Executive & Board-Level Risk Reporting · Risk Appetite & Tolerance Framing · Control Framework Design & Effectiveness Testing · KRI / KCI Metrics & Dashboards · Regulatory Engagement · PRINCE2 / Agile Delivery

Frameworks & Regulatory Compliance ISO 27001 · NIST CSF · NIS2 · PCI-DSS · GDPR · Maturity Assessments · Gap Analysis & Remediation Roadmaps

SOC, Threat Detection & Incident Response 24/7 SOC Operations Leadership · SIEM Engineering (Splunk, LogRhythm) · Threat Hunting · Incident Response Playbooks & Tabletop Exercises · Lessons-Learned Reviews · Resilience Planning

Offensive Security & Assessment Penetration Testing · Vulnerability Management · Breach Simulations · Red / Blue Team Exercises · Threat Modelling

Cloud & Infrastructure Security Azure Security · AWS Security · Multi-Cloud Risk Assessment · Cloud Migration Guardrails · Compensating Controls

Telecom Security eSIM Security Risk Assessment · Roaming & Interconnect Security · MVNO Operations · Third-Party Security Testing

Technical Skills Python · PowerShell · Bash · Firewalls · VPN · Network Monitoring · IAM / PAM Governance

PROFESSIONAL EXPERIENCE

Lebara Group — London, UK

Principal Information Security Engineer *(Security Expert)* · Sep 2025 – Present

- Lead enterprise and telecom security risk assessments across Lebara MVNO operations spanning the UK, France, Germany, Netherlands, and Denmark — governing control design, effectiveness testing, and regulatory alignment.
- Own end-to-end eSIM security risk assessments — encompassing threat modelling, control mapping, remediation tracking, and executive reporting across the full eSIM lifecycle.
- Serve as senior authority for roaming and interconnect security, overseeing third-party security testing and ensuring robust assurance across partner integrations.
- Support PCI-DSS and financial security governance for Lebara Money, embedding regulatory commitments into operational practice and control ownership.
- Produce executive risk registers and KPIs for leadership, providing C-suite visibility into cybersecurity risk posture and remediation progress.

Vodafone Group — London, UK

Cyber Security Senior Manager *(Cyber Security Expert)* · Jan 2018 – Sep 2025

- Led and mentored a multi-analyst security team across incident response, threat detection, and vulnerability management functions, building operational capability and maturity across multi-country environments.
- Directed 24/7 SOC operations encompassing threat hunting, SIEM engineering, IDS/IPS management, malware detection, SSL decryption, and packet analysis — establishing detection tuning and response standards.
- Delivered security assessments, breach simulations, and red/blue team exercises for banking and enterprise clients across EMEA, providing actionable remediation and proactive detection capabilities.
- Advised clients on control framework alignment to ISO 27001, PCI-DSS, and NIST CSF, embedding regulatory commitments into operational practice.
- Partnered with the CIISI-IE intelligence-sharing community — presenting on emerging threats and collaborating on cross-industry threat intelligence.

Vodafone — Cairo, Egypt

Cybersecurity Services Manager · Sep 2016 – May 2018

- Managed concurrent cybersecurity consulting engagements for financial and enterprise clients from RFP through delivery, spanning network security, vulnerability management, and compliance programmes.
- Delivered security assessments and remediation guidance against ISO 27001 and PCI-DSS, translating findings into prioritised, board-presentable roadmaps.
- Advised client security teams on incident-response capability, containment strategy, and recovery procedures.

E-Finance — Cairo, Egypt

Information Security Compliance Officer · May 2015 – Sep 2016

- Led financial-sector clients through ISO 27001 implementation and certification, owning gap analysis, control design, and remediation tracking.
- Conducted maturity assessments and developed remediation roadmaps aligned to industry frameworks and regulatory expectations.

EDUCATION

MSc Computer Science (AI & Security) — Ain Shams University, Cairo · 2021 – 2025

Thesis: *"Developing AI Secure Techniques for IoT in Healthcare."* Research published in peer-reviewed journals (see External Engagement).

BSc Computer Science — Egyptian Aviation Academy, Cairo · 2008 – 2012

CERTIFICATIONS

Leadership & Audit - CISA — Certified Information Systems Auditor *(in progress)* - PRINCE2 — Project Management Certification *(in progress)*

Technical Foundations eWPT (Web Application Penetration Testing) · eCPPTv2 (Professional Penetration Testing) · OSCP *(in progress)* · CCNA · Cisco CyberOps Associate · JNCIA-Cloud

EXTERNAL ENGAGEMENT & THOUGHT LEADERSHIP

Community - Active contributor to the **CIISI-IE** (Cyber Intelligence & Information Security Ireland) intelligence-sharing community — presenting on emerging threats and collaborating on cross-industry threat intelligence.

Publications - **Wiley Journal** — AI-secure techniques for IoT in healthcare. - **TELEMEDICINE Journal** — Secure AI-driven IoT healthcare systems.

Research focus: developing artificial intelligence techniques to secure Internet of Things (IoT) devices and data in healthcare environments.

LANGUAGES

- **English** — Fluent (Professional)
- **Arabic** — Native