Ahmed Adel Bakr Alderai

Incident Response & Threat Intelligence Leader

Dublin, Ireland | +353 89 618 0263 | ahmedalderai25@gmail.com | LinkedIn

Work Authorization: Stamp 4 (No sponsorship required)

Professional Summary

Incident Response and Threat Intelligence leader with **12+ years** driving security operations at enterprise scale. At Vodafone Group, directed breach investigations across **25+ countries**, led threat hunting operations that identified **APT activity**, and established detection engineering capabilities processing **500M+ security events daily**.

Core Expertise: Digital Forensics (Memory, Disk, Network) | Malware Analysis | Threat Actor Attribution | Detection Engineering | Cloud Security (AWS, Azure, GCP) | MITRE ATT&CK Mapping

Scaled SOC from **5 to 25 analysts** while reducing mean-time-to-contain (MTTC) by **75%** through SOAR automation and playbook development. Managed **$45M annual security budget**. Published researcher (Wiley) and conference speaker (Arab Security Conference, CCMIT18 Madrid).

Currently pursuing OSCP and GIAC certifications. Stamp 4 work authorization (no sponsorship required).

Key Achievements

Threat Detection & Response

- Led response to **sophisticated targeted intrusion** affecting telecom infrastructure across 6 countries, containing threat within 48 hours with zero confirmed data exfiltration
- Developed **200+ custom detection rules** (YARA, Sigma, Splunk) mapped to MITRE ATT&CK, achieving 85% technique coverage
- Reduced **mean-time-to-detect (MTTD) from 72 hours to 18 hours** through hypothesis-driven threat hunting program
- Achieved **80% reduction in vulnerability scores** through system hardening and refined detection processes

Security Operations & Leadership

- Scaled security operations team from **5 to 25 engineers** while managing $45M annual cybersecurity budget
- Processed **500M+ security events daily** across endpoint, network, and cloud telemetry with <15 minute SLA
- Implemented SOAR automation reducing manual alert triage by **40%** and false positive rate by 35%

Compliance & Industry Recognition

- Led security workstreams achieving **PCI DSS and ISO 27001 certifications** for systems processing $2B+ annually
- Represented Vodafone in **GSMA NESAS** (Network Equipment Security Assurance Scheme)
- **Published researcher** with peer-reviewed chapters in Wiley & Telemedicine on AI-driven security

Selected Investigations (Anonymized)

Telecom Infrastructure Intrusion (2022)

- **Scope:** Coordinated response to targeted intrusion affecting 6 operating companies
- **My Role:** Led technical investigation; performed memory forensics (Volatility), identified credential harvesting via Mimikatz, traced lateral movement through Zeek PCAP analysis
- **Outcome:** Contained within 48 hours; zero confirmed exfiltration; developed 12 new YARA signatures

Ransomware Outbreak Response (2020)

- **Scope:** Enterprise-wide ransomware affecting 2,000+ endpoints across 3 countries
- **My Role:** Directed IR team; reverse-engineered payload to identify kill switch; coordinated with law enforcement
- **Outcome:** 50% faster recovery than industry benchmark; $5M+ estimated loss prevention

Cloud Credential Compromise (2023)

- **Scope:** AWS IAM key exposure leading to unauthorized resource provisioning
- **My Role:** Analyzed CloudTrail logs; identified attack timeline; implemented IAM hardening playbook
- **Outcome:** Full remediation in 6 hours; no data loss; established new cloud IR procedures

---

Professional Experience

Cyber Security Assurance Expert Lead

Vodafone Group | London, UK | May 2018 – Present

Threat Intelligence & Detection Engineering

- Developed and maintained **YARA rules** and **Sigma rules** for detecting commodity malware, RATs, and APT tooling mapped to MITRE ATT&CK techniques
- Produced finished threat intelligence reports on emerging threats affecting telecommunications sector, distributed to 25+ operating companies
- Tracked **threat actor groups** targeting telecom infrastructure using **Diamond Model** and **Cyber Kill Chain** frameworks
- Created threat hunting hypotheses and executed weekly hunts across endpoint (EDR) and network (NDR) telemetry

Security Operations & Incident Response

- Lead frontline security operations analyzing real-time events across endpoint, network, and cloud using **Splunk Enterprise Security** and **LogRhythm**
- Direct incident management including escalations, resource allocation, and SLA compliance following **PICERL methodology**
- Perform host and network forensic analysis using **Volatility**, **EnCase**, and **Zeek** to understand attacker TTPs and assess business impact
- Execute static and dynamic malware analysis in sandbox environments to determine capabilities and develop detection signatures

Advanced Forensics & Cloud Security

- Conducted memory forensics investigations using **Volatility Framework** to identify fileless malware and credential harvesting

- Performed network forensics using **Zeek (Bro)** and full PCAP analysis to reconstruct lateral movement and C2 communications
- Led cloud security incident response across **AWS CloudTrail**, **Azure Activity Logs**, and **GCP Audit Logs** for compromised credentials
- Mapped detection coverage to MITRE ATT&CK framework, identifying gaps and prioritizing detection development roadmap

Leadership & Stakeholder Communication

- Scaled security team from 5 to 25 engineers, managing $45M annual budget for cybersecurity processes
- Acted as primary **security advisor to C-suite** during critical incidents, translating technical TTPs into business risk
- Authored **50+ incident reports** for executive and Board audiences with actionable remediation strategies
- Delivered **quarterly threat briefings** on emerging risks, security posture, and detection coverage KPIs
- Mentored 15 junior and mid-level analysts, with 3 promoted to senior positions

Security Engineering & Automation

- Spearheaded deployment of **CrowdStrike Falcon**, **Microsoft Defender ATP**, Nessus, and Qualys across enterprise
- Implemented **Cortex XSOAR** workflows automating alert enrichment, triage, and response playbooks
- Led DLP, DDoS Mitigation, and WAF integration projects achieving deployment under tight deadlines
- Represented Vodafone in GSMA Network Equipment Security Assurance Scheme (NESAS) influencing industry standards

Security Assurance & Cybersecurity Senior Analyst

Vodafone | Cairo, Egypt | Sep 2016 – May 2018

- Led incident response operations for ransomware and data breaches, improving time-to-recovery by 50%
- Conducted application and network penetration testing using Burp Suite, Metasploit, and custom scripts
- Reduced potential attack vectors by 40% through comprehensive vulnerability assessments
- Conducted 3 full-cycle IT risk audits covering networks, operating systems, databases, and security
- Created automated process to identify new devices and alert within 15 minutes of network connection
- Developed security awareness training programs, reducing recurring incidents by 15%

Compliance Officer

E-Finance | Cairo, Egypt | May 2015 – Sep 2016

- Lead consultant for two large **PCI DSS** compliance remediation projects handling $2B+ transactions
- Achieved successful **ISO/IEC 27001** and **PCI DSS** certification for card production systems
- Developed and implemented information security policies and procedures
- Led forensic investigations within regulated financial environment maintaining chain of custody
- Conducted internal audits against procedures, processes, and standards

Cybersecurity Trainee (Postgraduate Diploma)

Information Technology Institute (ITI) | Cairo, Egypt | Sep 2014 – May 2015

- Selected from **top 5%** of thousands of applicants for intensive 9-month cybersecurity program
- Comprehensive training in vulnerability management, penetration testing, incident response, and SOC operations

Junior Cyber Security Analyst

International Business Services (IBS) | Cairo, Egypt | Jan 2013 – Sep 2014

- Performed vulnerability management and incident response operations
- Implemented logging, reporting, and monitoring procedures for security events
- Delivered security awareness training across the organization

Technical Support Specialist

RESALA Training Center (RTC) | Cairo, Egypt | Sep 2009 – Jan 2013

- Built strong technical foundation supporting PC/Apple environments
- Implemented help desk procedures for logging, reporting, and monitoring

Technical Skills

Threat Detection & Hunting

- SIEM: Splunk Enterprise Security, LogRhythm, Google Chronicle (SecOps)
- Detection Engineering: **YARA**, **Sigma**, Snort/Suricata rules, custom correlation
- Threat Intelligence: MISP, ThreatConnect, Recorded Future, **STIX/TAXII**
- Network Monitoring: **Zeek (Bro)**, Suricata, Arkime, Wireshark
- Frameworks: **MITRE ATT&CK**, **Cyber Kill Chain**, **Diamond Model**, **PICERL**

Digital Forensics & Incident Response

- Disk Forensics: EnCase, FTK, Autopsy, X-Ways
- Memory Forensics: **Volatility**, Rekall, WinDbg
- Network Forensics: Wireshark, NetworkMiner, Zeek, full PCAP analysis
- Cloud Forensics: **AWS CloudTrail**, **Azure Activity Logs**, **GCP Audit Logs**
- IR Platforms: TheHive, **Cortex XSOAR**, Splunk SOAR, ServiceNow SecOps

Malware Analysis

- Static Analysis: PEStudio, YARA, strings, file entropy analysis
- Dynamic Analysis: Any.Run, Joe Sandbox, Cuckoo, Process Monitor
- Reverse Engineering: Ghidra (exposure), x64dbg
- Sandboxing: REMnux, FlareVM, custom isolated VMs

Endpoint & Cloud Security

- EDR/XDR: **CrowdStrike Falcon**, **Microsoft Defender ATP**, Carbon Black
- AWS: GuardDuty, Security Hub, CloudTrail, IAM Access Analyzer
- Azure: Microsoft Sentinel, Defender for Cloud, Azure Monitor
- GCP: Security Command Center, Chronicle SIEM, Cloud Armor

Scripting & Automation

- Languages: **Python**, **PowerShell**, **Bash**, C/C++ (reading)
- SOAR: Cortex XSOAR, Splunk SOAR, playbook development
- Automation: API integrations, IOC extraction, threat hunting scripts

Compliance & Governance

- Frameworks: ISO 27001, NIST CSF, NIST 800-53, CIS Controls v8
- Regulations: PCI DSS, GDPR, SOX, ITGC
- Standards: OWASP Top 10, GSMA NESAS, MITRE ATT&CK

Certifications

Security Operations & IR

- **Cisco CyberOps Associate** - SOC operations, threat analysis (2023)
- **ICS/SCADA Security 301V** - US DHS CISA Industrial Control Systems (2022)

Offensive Security & Penetration Testing

- **eCPPTv2** - Certified Professional Penetration Tester | INE (2021)
- **eWPT** - Web Application Penetration Tester | INE (2020)
- **OSCP** - Offensive Security | Exam scheduled Q1 2025

Networking & Cloud

- **CCNA** - Cisco Certified Network Associate (2019, renewed 2022)
- **JNCIA-Cloud** - Juniper Networks Cloud Associate (2023)

Management (Scheduled)

- **CISSP** - (ISC)² | Exam passed, endorsement pending (Expected Q1 2025)
- **GWAPT** - GIAC Web App Penetration Tester | Course enrolled (Q2 2025)

Education

Master of Science in Computer Science Ain Shams University, Cairo, Egypt | Oct 2024 – Sep 2026 (Expected)

- Thesis: *Developing AI-Driven Security Techniques for IoT in Healthcare*
- Published: “Mobile Doctor Brain AI App: AI for IoT Healthcare” (Wiley: ISBN 978-11-19509-87-5)

Postgraduate Diploma in Cyber Security Information Technology Institute (ITI), Cairo, Egypt | Sep 2014 – May 2015

Bachelor of Science in Computer Science Egyptian Aviation Academy, Cairo, Egypt | Oct 2008 – Jul 2012

- Grade: Very Good | Graduation Project: Excellent (AI-related)

Conference Speaking & Publications

- **Security BSides London** (2021): Teaching Assistant & Volunteer
- **Arab Security Conference**, Egypt (2021): Speaker - *“Be Part of the Future: Machine Learning & Cybersecurity”*

- **CCMIT18 Conference**, Madrid, Spain (2018): Speaker - *“Mobile Doctor Brain AI App: AI for IoT Healthcare”*
- **Published Chapter** in Wiley (ISBN: 978-11-19509-87-5)
- **Published Chapter** in Telemedicine (ISBN: 978-93-87500-35-8): *“Smart AI-IoT Healthcare Solution in Smart Homes Environment”*

Languages

- **English**: Fluent (Professional Working Proficiency)
- **Arabic**: Native