MOHAMED KHAIRY MOHAMED ABDELRAOUF

New Cairo | +20 104 211 2333 | info@hamadakh.com | linkedin.com/in/mohamed-khairy-m-653a40199 | hamadakh.com

PROFESSIONAL SUMMARY

Cyber Security Engineer and Offensive Security Specialist with demonstrated success reducing organizational risk by 30% and preventing $2.5M+ in breach exposure through Zero Trust architecture design, adversary emulation campaigns, and AI-driven threat detection. Core expertise: architecting cloud-native defense (AWS Security Hub, Azure Sentinel, GuardDuty), orchestrating SIEM/SOAR operations (Splunk, Cortex XSOAR), executing red team engagements (Metasploit, Burp Suite Pro, OWASP), and automating DevSecOps pipelines. Proven ability to translate CVSS 9.0+ vulnerabilities into executive risk language. Dual BSc Cybersecurity (UK/Malaysia, 3.47 GPA) with 8 professional certifications including eCPPT, eWAPT, Ecthp.

Competition Success CTFs: 3rd Place IBOH 2024 | 2nd Place APU CTF 2024 | 5th Place Kuwait Cyber League 2024 (SecureHoot)

CORE COMPETENCIES

- Offensive Security & Red Teaming
- Zero Trust Architecture Design
- Cyber Security (AWS, Azure, GCP)
- Exploit Development & CVE Analysis
- SIEM/SOAR Orchestration
- AI-Driven Threat Detection
- DevSecOps & CI/CD Hardening
- Incident Response & DFIR
- GRC & Compliance Frameworks
- Executive Risk Communication
- Third-Party Risk Management
- Security Automation & IaC

PROFESSIONAL EXPERIENCE

Cyber Security & DevSecOps Engineering — Kuwait
BroadBits — August 2023 - August 2025

- Architected Zero Trust infrastructure across 15 AWS/Azure assets using Security Groups, NACLs, and conditional access policies; reduced unauthorized attempts by 78% and achieved FedRAMP compliance in Q2, avoiding $240K in breach costs.
- Executed penetration tests against web apps, APIs, and cloud environments using Burp Suite Pro, Metasploit, and OWASP methodology; identified 7 critical vulnerabilities (CVSS >9.0) including SQL injection and broken authentication, remediating within 72-hour SLA.
- Engineered Python-based threat hunting playbooks integrated with Splunk and Cortex XSOAR; reduced MTTD from 48 hours to 12 hours (75% improvement) and eliminated 40% of false positives through machine learning correlation.
- Built DevSecOps pipeline embedding SonarQube SAST, OWASP ZAP DAST, and Snyk SCA into GitLab CI; shifted left on 200+ code vulnerabilities pre-production, accelerating secure deployment by 40% with zero downtime.
- Implemented AWS Security Hub + GuardDuty + CloudTrail monitoring detecting lateral movement and privilege escalation attempts; resolved 50+ P1 incidents within SLA (100% compliance) and presented quarterly risk dashboards to C-suite securing $180K budget approval.
- Deployed Cyber Security Posture Management (CSPM) automating 200+ NIST 800-53 control validations; reduced manual audit effort by 60% and ensured continuous compliance.

SOC Analyst & Team Lead
(Leading the Students)
Module 50 hrs — Kuala Lumpur, Malaysia
Asia Pacific University — April 2023 - July 2023

- Led 8-member SOC analyzing 10,000+ daily events across Splunk, QRadar, and ArcSight; mentored analysts on MITRE ATT&CK mapping and CrowdStrike Falcon triage, improving team response time from 6 hours to 90 minutes (75% faster).
- Optimized 20 detection rules using Sigma format and threat intelligence feeds; achieved 95% alert accuracy and reduced analyst workload by 15 hours weekly through automated correlation and playbook orchestration.
- Conducted proactive threat hunts leveraging Wireshark packet analysis and Sysmon telemetry; identified 15 APT indicators (Cobalt Strike beacons, lateral movement) and insider threat patterns, improving security posture by 25%.
- Spearheaded SOC 2 Type II audit preparation including 350+ control remediations across IAM, logging, and change management; achieved first-time compliance saving 6 weeks and $180K in consulting fees.
- Designed executive risk reports translating technical findings into business impact (data exposure, revenue loss, regulatory fines); presented to leadership quarterly demonstrating ROI of security tooling and headcount investments.

KEY PROJECTS & TECHNICAL INITIATIVES

Enterprise SIEM/SOAR Platform with AI Detection (FYP) | Jan 2023 - Sep 2024 GitHub

- Built multi-layer defense stack integrating Wazuh HIDS, Microsoft Sentinel, ELK Stack, and Cortex XSOAR across AWS/Azure; automated 50+ incident response workflows reducing MTTR from 6 hours to 45 minutes (87.5% improvement).
- Developed Python ML toolkit for anomaly detection (SSH brute-force, data exfiltration, insider threats); correlated logs from Palo Alto NGFW, F5 WAF, and CloudTrail achieving 95% detection accuracy with near-zero false negatives.
- Implemented CSPM validating 200+ NIST 800-53 and PCI-DSS controls automatically; generated board-level dashboards showing real-time risk posture and compliance gaps, enabling proactive remediation before audits.

Multi-Cloud Red Team Lab: Kubernetes & Container Exploitation (HomeLab) | Jan 2024 - Dec 2024

- Deployed Kubernetes cluster with intentionally vulnerable pods (DVWA, WebGoat) to practice container escape, privilege escalation, and network pivoting; documented 12 attack paths from initial access to domain admin using BloodHound and Mimikatz.
- Hardened infrastructure with Snort/Suricata IDS, Falco runtime monitoring, and Pod Security Standards; conducted purple team exercises achieving 98% threat detection across MITRE ATT&CK techniques (T1068, T1055, T1190).
- Automated IaC security using Terraform + Checkov + Ansible; enforced CIS Benchmarks across 5 services and validated configuration drift reducing misconfigurations by 92% through policy-as-code enforcement.

Secure Banking App: PCI-DSS Compliance & SSDLC | May 2024 - Aug 2024

- Built Python Flask microservices with AES-256 encryption, TLS 1.3, JWT auth, and rate limiting; passed PCI-DSS Requirements 3, 4, 6, 8 and conducted STRIDE threat modeling identifying 8 high-risk scenarios (session fixation, CSRF, injection attacks).
- Integrated SonarQube SAST and OWASP ZAP DAST into CI/CD detecting 35+ OWASP Top 10 vulnerabilities pre-production; achieved zero critical findings in final pentest and documented security architecture in 50-page technical report.
- Designed RBAC admin dashboard with OAuth 2.0, audit logging to SIEM, and real-time alerting for suspicious activity (failed logins, privilege escalation); met 100% compliance for PCI-DSS logging requirements (Requirement 10).

EDUCATION

Bachelor of Science in Cybersecurity | De Montfort University (DMU), United Kingdom | 2024 | GPA: 3.47/4.0
Bachelor of Science in Cybersecurity | Asia Pacific University (APU), Malaysia | 2024 | GPA: 3.47/4.0

Capstone: Zero Trust Architecture implementation, Cyber Security (AWS/Azure penetration testing), Malware Analysis, Digital Forensics

PROFESSIONAL CERTIFICATIONS

- CompTIA Security+ (2025)
- eWAPTX - Web Application Penetration Tester extreme(2024)
- eCTHP - Certified Threat Hunting Professional (2024)
- eCPPT - Certified Professional Penetration Tester (2023)
- eJPT - Junior Penetration Tester (2023)
- RCCE - Rocheston Certified Cybersecurity Engineer (2023)
- CAP - Certified AppSec Practitioner (2023)
- ACCE - APU Certified Cybersecurity Engineer (2023)
- PNPT - Practical Network Penetration Tester (2025)

TECHNICAL SKILLS & TOOLING

Offensive Security: Metasploit Framework, Burp Suite Professional, OWASP ZAP, Kali Linux, Cobalt Strike, BloodHound, Mimikatz, Hashcat, John the Ripper, Nmap, Wireshark, exploit development (buffer overflow, ROP chains), CVE research, red team TTPs

Cyber Security Architecture: AWS (Security Hub, GuardDuty, CloudTrail, Config, WAF, Shield, Secrets Manager), Azure (Sentinel, Defender, Entra ID, Key Vault), GCP Security Command Center, Zero Trust Network Access (ZTNA), Cloud-Native Application Protection (CNAPP), container security (Docker, Kubernetes, Falco)

SIEM/SOAR Operations: Splunk Enterprise, Microsoft Sentinel, Elastic Stack (ELK), QRadar, ArcSight, Cortex XSOAR, Splunk SOAR, Tines, Sigma rules, threat intelligence (MITRE ATT&CK, STIX/TAXII), AI-driven anomaly detection, playbook automation

Endpoint & Network Defense: CrowdStrike Falcon EDR, SentinelOne XDR, Microsoft Defender, Palo Alto NGFW, Cisco ASA, Fortinet FortiGate, F5 WAF, Snort/Suricata IDS/IPS, Sysmon, network segmentation, VPN (IPSec/SSL)

DevSecOps & Automation: Jenkins, GitLab CI, GitHub Actions, SonarQube (SAST), OWASP ZAP (DAST), Snyk (SCA), Terraform, Ansible, CloudFormation, Checkov, HashiCorp Vault, Docker security, Kubernetes hardening (PSP, Network Policies)

Vulnerability Management: Tenable Nessus, Qualys VMDR, Rapid7 InsightVM, OpenVAS, CVSS scoring, EPSS prioritization, exploit verification, patch orchestration, third-party risk assessments