

ALGHALIAH TAJ A.

Saudi Arabia & United Kingdom | +966 555 876 104 | +44 774 857 2981 | alghaliah.taj@outlook.com
LinkedIn: linkedin.com/in/alghaliah-taj-a-987607352 | Portfolio: alghaliahtaj27.github.io

PROFESSIONAL SUMMARY

First Class Honours graduate in Cybersecurity and Forensic Computing (BSc Hons, GPA 3.6/4.0, University of Portsmouth, 2026) with demonstrated hands-on capability across malware reverse engineering, OSINT-driven threat detection, penetration testing, vulnerability research, and IoT security. Built and evaluated a four-layer OSINT framework using a Random Forest classifier to detect fraudulent cryptocurrency websites, achieving 91.4% accuracy and 92.9% precision across 875 real-world URLs. Conducted full static, dynamic, and reverse-engineering analysis of live malware, uncovering IRC-based command-and-control infrastructure, registry persistence, and screen-capture spyware behaviour. Designed and deployed CyberLight, a low-cost hardware device that detects and physically visualises live network attacks in real time. Completed a cybersecurity internship in Saudi Arabia. Native Arabic speaker with advanced English (IELTS certified) and intermediate Turkish, combining strong technical depth with regional and cultural fluency across the UK and Saudi markets. Actively seeking an entry-level SOC Analyst, Security Analyst, Digital Forensics Investigator, Penetration Tester, or GRC Analyst role.

EDUCATION

BSc (Hons) Cybersecurity and Forensic Computing — University of Portsmouth | **First Class Honours** |
GPA: 3.6 / 4.0 2022 – 2026

Key Module Results (Final Year):

- **Practical Data Analytics and Mining: 83% — First Class** (feature engineering, ML model selection, Random Forest, evaluation metrics)
- **Vulnerability Discovery and Exploitation: 80% — First Class** (penetration testing portfolio, CVE mapping, exploitation techniques)
- **Ethical Hacking: 77% — First Class** (coursework), 75% (oral assessment and presentation)
- **Cyberlaw, Governance and Human Rights: 72% — First Class** (legal and regulatory frameworks, data protection)
- **Final Year Dissertation — CIOF Framework: 72% — First Class** (91.4% ML classifier accuracy across 875 URLs)

Relevant modules: Digital Forensics, Ethical Hacking, Cyber Threat Intelligence, Incident Response, Business Information Security Systems, CyberLaw Governance and Human Rights, Operating Systems and Internetworking, Internet of Things.

Cambridge International A-Level and IGCSE 2019 – 2021

Top grades in Science and Mathematics.

TECHNICAL SKILLS

Malware Analysis and Digital Forensics: IDA Pro, PEiD, UPX/packer analysis, Wireshark, RegShot, Process Monitor, Volatility, memory and disk imaging, certutil, x86 Assembly reverse engineering

Penetration Testing and Vulnerability Research: Nmap, Metasploit Framework, Google dorking, OSINT reconnaissance, DVWA, Nessus vulnerability scanning, Burp Suite, OWASP Top 10, CVE analysis

Programming and Scripting: Python (pandas, scikit-learn, Requests, BeautifulSoup, Scapy), Bash, PowerShell, x86 Assembly, regex, SQL

OSINT and Threat Intelligence: WHOIS, DNS, SSL infrastructure analysis, MITRE ATT&CK framework, blockchain and wallet tracing, GDPR-compliant risk scoring, social media OSINT

Security Operations and Networking: Incident response, network hardening, SIEM concepts, log analysis, network protocol analysis, TCP/IP, firewall fundamentals

IoT and Embedded Security: Arduino, Raspberry Pi, MQTT over TLS, Scapy packet analysis, edge device security

Governance, Risk and Compliance: ISO 27001 awareness, NIST framework, GDPR, Saudi PDPL, risk assessment, security policy development

KEY PROJECTS

Cryptocurrency Investigative OSINT Framework (CIOF) — Final Year Dissertation | 72% — First Class 2026

- Designed a four-layer OSINT framework (infrastructure, on-site content, social footprint, blockchain) to investigate fraudulent cryptocurrency websites.
- Trained a Random Forest classifier (scikit-learn) on 875 real labelled URLs achieving **91.4% accuracy**, 92.9% precision, and a 0.925 F1-score.
- Cross-referenced extracted wallet addresses against the Real-CATS dataset of 90,000+ flagged criminal cryptocurrency addresses.
- Produced graduated risk classifications (Legitimate / Suspicious / Scam) with inspectable, evidence-based output rather than black-box verdicts.
- Addressed a £9.39 billion annual global problem with a practically deployable, analyst-friendly detection tool.

Malware Forensic Investigation — Simulated Insider Threat Case | First Class 2025

- Performed static analysis in IDA Pro on a UPX-packed sample, identifying hardcoded C2 infrastructure, persistence mechanisms, and anti-analysis strings.
- Validated findings dynamically: Wireshark confirmed IRC-based C2 traffic; RegShot proved registry-based persistence.
- Reverse-engineered binary to map specific API calls (RegSetValueExA, InternetOpenA, BitBlt) to persistence, C2, and screen-capture spyware behaviour.

- Delivered a full indicator-of-compromise list and a remediation and hardening plan for the simulated client.

CyberLight — IoT Network Attack Visualisation System — | First Class 2026

- Built a low-cost (~£37) Arduino-based device that turns invisible network attacks into physical alerts via LED, LCD display, and buzzer.
- Wrote a Python/Scapy monitoring layer to detect port scans, rogue devices, brute-force logins, and unencrypted services in real time.
- Published all detection events to a cloud MQTT broker over TLS, providing a persistent, remotely accessible audit log.
- Demonstrates practical understanding of IT/OT convergence and physical security layer integration.

Practical Penetration Testing and Vulnerability Research — | 80% — First Class 2025

- Remediated a command-injection vulnerability in a PHP DNS lookup tool by replacing unsafe shell execution with validated, native function calls.
- Used Google dorking for OSINT reconnaissance, identifying exposed credentials and admin login pages on test infrastructure.
- Exploited a file-upload vulnerability to establish a reverse shell via Netcat against a deliberately vulnerable web application.
- Mapped three real-world WooCommerce CVEs (SQL injection, XSS, broken access control) to the OWASP Top 10 with code-level mitigations.
- Completed a TryHackMe CTF end-to-end, covering reconnaissance, exploitation, and privilege escalation, capturing both user and root flags.

PROFESSIONAL EXPERIENCE

Cybersecurity and Information Systems Intern — Vision Energy Industrial LLC Jun – Aug 2025

Dammam, Saudi Arabia | Hybrid

- Supported day-to-day system and network security operations within a Cybersecurity and Information Systems team at a Saudi industrial organisation in the energy sector.
- Assisted with security monitoring, log analysis, and threat identification activities to detect and escalate potential vulnerabilities across the organisation's infrastructure.
- Contributed to internal security projects, policy implementation, and staff security awareness initiatives alongside senior cybersecurity professionals.
- Gained practical exposure to OT-adjacent network environments and industrial cybersecurity operations in a real-world energy sector setting.

AWARDS AND ACHIEVEMENTS

First Class Honours — BSc (Hons) Cybersecurity and Forensic Computing, University of Portsmouth, 2026

GPA 3.6 / 4.0 — Consistent First Class performance across final year modules including 83% in Data Analytics, 80% in Vulnerability Discovery and Exploitation, and 77% in Ethical Hacking

First Class Dissertation — CIOF framework achieved 91.4% ML classifier accuracy; independently designed, built, and evaluated with no prior template

First Class Hardware Project — CyberLight IoT device independently designed, built, and deployed for real-time network attack detection

CERTIFICATIONS AND PROFESSIONAL DEVELOPMENT

CompTIA Security+ — Currently studying (2026)

Certified Ethical Hacker (CEH) — Planned

TryHackMe — Active platform user, CTF completion and structured learning paths

Independent Research — Conducting two-part research series on Arabic-language phishing detection gaps affecting 300M+ Arabic speakers

LANGUAGES

Arabic — Native | **English** — Advanced (IELTS certified) | **Turkish** — Intermediate