IRFAN MEHTAB HUSSAIN

Telephone Number: +44 7842 478598   Email Address: iru.hussain4@gmail.com
LinkedIn: www.linkedin.com/in/irfan-hussain045

EDUCATION

King's College London (2024 – Present)

- Master's Degree in Computer Science - Predicted First Class
- ISACA Digital Trust Scholarship (2025) - Awarded for excellence and commitment to cybersecurity

Trinity School, Croydon (2017 – 2024)

- A Levels - Further Mathematics (A*), Computer Science (A*), Mathematics (A*), Physics (A)
- GCSEs - 8 × Grade 9 (including Further Mathematics), 3 × Grade 8

SKILLS & CERTIFICATIONS

- **Certifications** - CompTIA Security+ (Oct 2025), Google Cybersecurity Professional Certificate (Sep 2025)

- **Programming & Scripting** - Python, C++, Java, Scala, Django, HTML, CSS, Tailwind, JavaScript, TypeScript, Next.js, Git, SQL, KQL, SPL, Power Automate (WDL)

- **Cybersecurity Tools & Platforms** - Wireshark, Nmap, Suricata, Splunk, Microsoft Sentinel, CrowdStrike, Microsoft Defender, QRadar, XSOAR, Linux, GitHub

WORK EXPERIENCE

Security Operations Centre Internship – BT Group, Belfast (June 2025 – Aug 2025)

- Took initiative to develop triage and investigation automation using Microsoft Power Automate, HTML/CSS, Falcon Sandbox API, and OpenAI, reducing manual work and saving 1,000+ analyst hours per year (~£40,000)
- Engineered 11 Splunk detections aligned with MITRE ATT&CK, designing queries with optimal thresholds and dependency management to improve alert coverage
- Developed a Splunk dashboard monitoring Scattered Spider activity across 7 key attack behaviours, enabling proactive threat detection with clear visualisations
- Built and optimised 10+ playbooks in Sentinel (using KQL) and Splunk (using SPL), standardising alert response and increasing SOC efficiency
- Resolved 50+ alerts across Microsoft Sentinel/Defender, Splunk, QRadar, XSOAR, and CrowdStrike, becoming the only intern to handle all onboarded platforms
- Presented projects to SOC team and senior managers, demonstrating technical innovation, operational impact, and professional communication

Cybersecurity Auditing Shadowing – BNY Mellon, Pittsburgh (Aug 2022)

- Assessed risk management and mitigation techniques, including honeypots and intrusion detection systems, under the Head of Cybersecurity Auditing
- Observed audit meetings for new vulnerability detection software, reviewing processes and questioning development teams to understand real-world auditing workflows

Online Cybersecurity Work Experience - Telstra & ANZ (2023)

- **Telstra (Dec 2023)** - Investigated simulated phishing attempts and reviewed firewall logs to identify attack patterns, coding Python-based firewall rules to filter malicious traffic accordingly
- **ANZ (May 2023)** - Operated as a virtual security analyst using Wireshark to inspect network traffic, trace suspicious activity, and document findings for post-incident investigations

EXTRACURRICULARS AND ACHIEVEMENTS

- **Advanced Coding Club (Founder & Leader, 2023–2024)** - Designed weekly coding challenges (e.g., sudoku solvers, cryptarithmetic decoders) and mentored 50+ peers in complex algorithms

- **Geek-O-Lympics 2nd Place (2023)** - Created an AI-powered exercise assistant using Mediapipe and data visualisation to analyse bicep curls, track progress, and provide real-time feedback

- **Industrial Cadets Silver Award (2023)** - Presented a fluid dynamics project using the Lattice-Boltzmann Method, earning an award for applied mathematics and computational skills

- **IBM Basic Network and Database Security MOOC (2022)** – Gained a deeper understanding of network protocols, databases, SQL, injection threats, and enterprise data protection

- **Volunteer Experience** - Supported children with complex needs at Rutherford School (2023) and assisted with retail and fundraising at the British Heart Foundation (2022–2023)