## Muhammad Subhan Nizal

Contact: 07444 681 779 | [Subhan05@hotmail.co.uk](mailto:Subhan05@hotmail.co.uk) | Nottingham, UK

## Professional Summary

Driven and detail-oriented professional with a strong foundation in fundraising, sales management, and growing expertise in cybersecurity. Proven ability to exceed targets through innovative strategies, effective leadership, and top-notch communication skills. Highly organized and adaptable, with hands-on experience in network security and a keen interest in safeguarding digital systems. Ready to apply technical skills and resilience to excel in cybersecurity analyst roles; Bringing hands-on experience in network security— including firewall configuration, AAA authentication, and network troubleshooting via Cisco Packet Tracer—alongside a Level 3 Diploma in Networking and Cybersecurity. Combines strong organisational skills, resilience from amateur boxing, and a proactive approach to learning, positioning me as a dedicated candidate ready to excel in protecting digital infrastructures and mastering advanced IT systems.

Fundraising Representative  
Nottingham | Nov 2023 – Feb 2024

* Led and coordinated teams for community fundraising initiatives, managing logistics across Nottingham.
* Engaged with over 100 households daily, consistently enrolling an average of 3 new donors per day, surpassing enrolment targets by 20%.
* Developed and implemented persuasive sales techniques, enhancing adaptability and performance in challenging environments.
* Delivered motivational presentations at team meetings, resulting in a 10% increase in overall team performance.
* Maintained high team morale and commitment during long hours and adverse weather conditions.
* Spearheaded projects that improved operational efficiency by 15%.

## Education

Bluecoat Wollaton Academy, Nottingham  
GCSEs | Sep 2017 – Sep 2021

* Mathematics: Grade 5
* English: Grades 4 & 5
* Combined Science: Grades 6/5
* Geography: Grade 5
* History: Grade 4
* Religious Education: Grade 5

Certifications

* Level 2 Certificate in Digital and IT Skills
* Level 1 Certificate in Digital Contact Centre
* Level 1 Award in Cybersecurity
* Level 3 Diploma in Networking and Cybersecurity.

## Skills

* IT literacy: Proficient in Microsoft Word and Excel
* Customer service excellence
* Cybersecurity fundamentals
* Sales and fundraising strategy
* Team leadership and motivation
* Strong communication and presentation

## Interests

* Amateur Boxing: Training intensively for competitive bouts under England Boxing. Developed discipline, resilience, strategic thinking, and determination.
* Research: Enthusiastic about neurochemistry, nutrition, nootropics, and herbal supplements.

## Cybersecurity Projects

***Access Control & AAA Authentication Implementation Project:***  
Level 3 Diploma in Cybersecurity & Networking, B2W Group

* Configured and managed AAA (Authentication, Authorization, and Accounting) authentication on Cisco routers and servers within a simulated enterprise environment for “Pentest Ground.”
* Created and enforced local user accounts and implemented secure password policies, enhancing access control for network devices.
* Set up and verified console access authentication using a local database, ensuring only authorized users could access network infrastructure.
* Conducted end-to-end connectivity testing across multiple network segments, troubleshooting and resolving configuration issues to maintain network integrity.
* Documented all configurations and validation steps, including user access verification and Telnet authentication, demonstrating strong attention to detail and technical communication skills.

***Pentest Ground Website Security Assessment and Risk Mitigation Project:***

* The project for the Pentest Ground Website Security Assessment and Risk Mitigation involves several key phases: project planning, reconnaissance and information gathering, scanning, reporting, and resource management. Team members are assigned specific tasks, such as confirming the project scope and finalizing roles. In the reconnaissance phase, scanning tools will be used to identify open ports and services, with findings recorded for later testing. The scanning phase focuses on using automated tools to detect vulnerabilities, highlighting critical issues. Moving into the reporting phase, the team is required to summarize vulnerabilities, provide detailed findings, and recommend improvements to security policies. Throughout the project, resources like testing tools and hardware are allocated properly, while stakeholders are updated regularly to track progress. Regular interim reviews are scheduled to discuss updates, address issues, and ensure that timelines are adhered to.

***Network Configuration and Documentation Project:***

***Independent Study | Via Level 3 Diploma in Networking and Cybersecurity***

* Designed and documented a secure network setup, focusing on configuring switches, routers, and servers in a simulated environment, supported by detailed screenshots.
* Implemented VLAN configurations and verified traffic isolation to enhance network segmentation and security.
* Performed system diagnostics and connectivity tests, troubleshooting issues to ensure optimal performance, with results captured in comprehensive reports.
* Compiled a detailed project portfolio with annotated screenshots, showcasing technical accuracy and readiness for real-world cybersecurity tasks.

***Automated security log monitoring project:***

Designed and implemented a Python-based automated security log monitoring solution on Windows, leveraging Windows Event Log APIs to detect suspicious activity such as failed login attempts. The project involved writing and customizing a script to parse security logs, identify key threat indicators (e.g., Event ID 4625), and alert the user through both console output and Windows pop-up notifications. I configured and tested the automation in a real environment by scheduling the script to run at set intervals using Windows Task Scheduler, ensuring continuous and hands-off security event monitoring. This project demonstrates my ability to automate cybersecurity tasks, perform log analysis, and deliver practical solutions using Python on enterprise platforms.

***AI Email Phishing Detector Project— Python, Machine Learning, GUI:***

Developed a full-stack AI-powered phishing detection tool that connects to email inboxes using IMAP, leverages advanced open-source NLP models (DistilBERT) to classify emails as phishing or legitimate, and safely handles long inputs through model-specific truncation. Built a user-friendly Tkinter GUI enabling easy one-click inbox scanning and flagged email visualization. Automated the workflow using Windows Task Scheduler for routine scanning.

This project demonstrates:

End-to-End Python Engineering: Designed and implemented the entire solution, from backend data handling and model integration to robust error management and automation.

Advanced Natural Language Processing: Leveraged state-of-the-art, open-source NLP models (DistilBERT) for real-time phishing classification, including optimized token management and input preprocessing for consistent, high-accuracy predictions.

Cybersecurity Awareness & Application: Developed proactive threat-detection logic, adhering to best cybersecurity practices around safe email handling, credential management, and risk mitigation.

User-Centered Desktop App Development: Built an intuitive, cross-platform graphical interface with Tkinter, empowering non-technical users to scan inboxes with a single click and instantly visualize flagged threats.

Automation & Operational Reliability: Integrated the solution with Windows Task Scheduler to enable seamless, unattended background scanning for continual protection.

IMAP Email Protocol Mastery: Securely interfaced with email inboxes using IMAP, efficiently parsing messages, attachments, and metadata—including support for bulk/filtered scans.

Collaborative Coding & Documentation: Delivered maintainable code with clear structure, documented usage in a well-organized README, and demonstrated readiness for team collaboration or open-source distribution.

Continuous Improvement Mindset: Explored features like logging, hybrid detection (AI and rule-based), and instant user notifications for a complete, enterprise-relevant solution.

***AI-Powered and Automated Cybersecurity Activity Blog Project:***

Successfully designed and automated a comprehensive, AI-powered cybersecurity activity blog that documents and showcases professional development. Engineered an end-to-end workflow that integrates ActivityWatch for detailed activity tracking, Python scripts for log processing and project documentation, and a local LLM (using Ollama) for generating daily technical reflections in clear, professional language. Deployed a static portfolio site with MkDocs and GitHub Pages, ensuring updates are automatic and maintenance-free.

Key Achievements:

Built a hands-off workflow that tracks daily cybersecurity activities, classifies them by relevance, and generates articulate blog posts highlighting technical skills and project milestones.

Automated the aggregation and summarization of key projects, providing recruiters with clear, up-to-date evidence of technical growth and leadership in cyber automation.

Deployed, scheduled, and maintained the process using Windows automation tools, demonstrating strong abilities in DevOps, scripting, task scheduling, and site deployment.

Demonstrated initiative and innovation by integrating AI summarization, self-documenting progress, and creating a dynamic technical portfolio for career advancement.

This project highlights advanced skills in automation, scripting, machine learning integration, and self-driven documentation, directly supporting professional visibility and credibility in cybersecurity.