

Jash Vaidya

Security Operations Analyst

London, UK | +44 7741260445 | jashvaidya.cyber@gmail.com | [LinkedIn](#) | [Github](#) | [TryHackMe](#)

Cybersecurity Analyst | CompTIA Security+ | Proficient in threat detection, vulnerability management, and security frameworks including NIST and MITRE ATT&CK. Hands-on experience with security tools including Splunk, Wireshark, and Nessus for comprehensive security operations.

PROFESSIONAL EXPERIENCE

Metbrains

London, UK

Cybersecurity Intern (Blue Team Focus)

December 2025-Present

- Directed SOC triage: Managed SIEM alerts (Splunk/Sentinel), tuning detection rules to reduce noise and focus on high-fidelity, actionable threats.
- Conducted incident forensics: Leveraged Wireshark for deep packet capture (PCAP) and log correlation to map attacker activity and determine root cause.
- Supported vulnerability management: Deployed Nessus/Nmap scans, analyzing and prioritizing critical weaknesses across systems for immediate remediation.
- Enhanced defense posture: Applied system hardening in Linux environments and mapped operational controls to the MITRE ATT&CK framework.

Opstalent

Wrocław, Poland

Senior Customer Service Representative

February 2022-June 2023

- Resolved 326+ monthly escalated cases for enterprise clients (Amazon, Nike, ZARA), achieving a 90% resolution rate and top-tier CSAT scores.
- Trained 10+ agents in security-aware customer support, reducing account breaches by 15% via phishing detection protocols.
- Awarded "Second Best Customer Service Representative" in 2023 across the organisation for outstanding performance and client feedback.

Customer Service Representative

February 2021-February 2022

- Demonstrated strong security awareness by properly handling sensitive customer data and following strict authentication protocols for account access requests.

SKILLS

Technical Skills & Tools: Network Security, Firewalls, IDS/IPS, TCP/IP Networking, Vulnerability Management, Threat Intelligence, Incident Response, Log & Packet Analysis, Endpoint Protection, Risk Assessment, Penetration Testing Fundamentals, MITRE ATT&CK, SIEM (Splunk, Elastic SIEM, Microsoft Sentinel), EDR/XDR (CrowdStrike Falcon, SentinelOne), Wireshark, OSINT tools (VirusTotal, AbuseIPDB, WHOIS/DNS lookup), phishing analysis tools (PhishTool, email header analyzers), ticketing/ITSM (Jira, ServiceNow), vulnerability scanners (Nessus, OpenVAS), log management (Elastic Stack/ELK), Linux networking tools (tcpdump, nslookup, dig), PCI DSS, Regex, Scripting.

Soft Skills: Analytical Thinking, Communication, Teamwork, Adaptability, Continuous Learning.

CERTIFICATIONS

[Microsoft Certified: Azure Fundamentals](#) | November 2025

[CompTIA Security+](#) | June 2025

[Cisco Cybersecurity Essentials](#) | Dec 2022

[Cisco CCNA](#) | Mar 2021

CEH | In Progress | Feb 2026

(ISC)² CC | In Progress

ITIL Foundation

EDUCATION

University of West London | London, UK

September 2023–September 2024

MSc Cyber Security, Graduated with Merit (2:1)

Relevant Modules: Cyber Analysis, Network and Systems Security, Security Operations and Assurance, Big Data Analysis, Machine Learning.

- Applied core security methodologies across a diverse curriculum, including SOC simulation (Splunk/Wireshark), vulnerability management (Nessus, Metasploit), and secure network architecture design (Pfsense, ACLs).
- Developed expertise in advanced security analysis leveraging coursework in Big Data and Machine Learning.
- Dissertation: Global Routing Optimization using BGP.

University of Information Technology and Management | Rzeszow, Poland

September 2019–July 2023

BSc IT, Graduated with First-Class Honours

Relevant Modules: Network Fundamentals, Systems Administration, IT Security Principles.

- Developed foundational expertise in IT infrastructure and system administration, implementing Active Directory and VMware environments, and automating core tasks using PowerShell and Bash scripting across Windows and Linux systems.
- Thesis: Virtual Business Card generator

ADDITIONAL

Languages: Hindi (Fluent), English (Fluent), French (A1), Polish (A1).

Portfolio: [Github](#)

Training Platforms: [TryHackMe](#)