

DELBIN JOSEPH

COMPTIA SECURITY+ CERTIFIED

+91 9207099714 | hello@delbinjoseph.com | Kerala, India | delbinjoseph.com | linkedin.com/in/delbinjoseph

OBJECTIVE

CompTIA Security+ certified, transitioning into cybersecurity from a background in IT support. Built a home SIEM lab covering FIM and MITRE ATT&CK mapping, alongside on-the-job experience with DNS, email security, and internal automation. Looking for an entry-level cybersecurity role to keep building on this foundation.

CERTIFICATIONS

CompTIA Security+ (SY0-701) | CompTIA, March 2026
verify.comptia.org | code: 0f975eb454b743589997b478e4dfdcf3

PROJECTS

Wazuh SIEM Home Lab

- Deployed a multi-OS Wazuh SIEM with real-time file integrity monitoring on Windows and Linux.
- Wrote a custom detection rule mapped to MITRE ATT&CK to flag suspicious executable drops.
- Added Sysmon for process visibility and traced a high-severity alert to its root cause.
- Simulated an SSH brute-force attack with MITRE-mapped detection and automated IP blocking.
- Investigated and documented false positives, including one from the monitoring tool itself.

EDUCATION

Master of Science, Information Security, Indira Gandhi National Open University *2026 – Present*

Bachelor of Commerce, Computer Applications, University of Calicut, Alphonsa College Thiruvambady
2019 – 2022

PROFESSIONAL EXPERIENCE

IT Support & Accounts Executive, Jaffah Dates & Nuts *Dec 2022 – Present*

- Managed company domain migration to Cloudflare, configuring DNS records, SPF, DKIM, and DMARC email authentication.
- Identified company owner's personal contact information exposed in public WHOIS records and ensured privacy protection was enabled during the domain migration.
- Built internal automation tools using Google Sheets, AppSheet, and AppScript to improve workflow efficiency across multiple office branches.
- Progressed from a pure accounting role to managing IT infrastructure, security configurations, and automation tools, demonstrating initiative and self-directed technical growth.

CORE SKILLS

Security: Threat Detection, Alert Triage, Networking Fundamentals, OSINT, Email Security, Problem Solving, Attention to Detail

General Technical: Linux CLI, Windows, DNS Management, Cloudflare, Google Sheets, AppSheet, Google AppScript