

RICHU JOSEPH

Kottayam, Kerala, India | richujoseph201@gmail.com

modern.richujoseph.in | linkedin.com/in/richujoseph | github.com/richujoseph | tryhackme.com/p/richujoseph

Summary

Final-year Cyber Security undergraduate with industry experience validating enterprise EDR, NDR, XDR and SIEM/SOAR products against MITRE ATT&CK. Hands-on with adversary emulation, detection validation and Python security automation. Seeking SOC, detection engineering or security testing roles from 2027.

Education

St. Joseph's College of Engineering and Technology (SJCET), Palai
B.Tech, Computer Science and Engineering (Cyber Security) — CGPA 7.63/10

Kerala, India
Oct 2023 – Jun 2027

Experience

Cyber Security Intern — Security Product Testing
Algomox Pvt. Ltd.

May 2026 – Jul 2026
Bengaluru, Karnataka

- Performed black-box validation of enterprise EDR, NDR, XDR and SIEM/SOAR products against MITRE ATT&CK.
- Ran adversary emulation with Atomic Red Team, PowerShell, Bash and custom attack simulations on Windows and Linux.
- Measured detection coverage, analysed security events and documented detection gaps as reproducible test cases.
- Automated repetitive validation workflows in Python and Playwright, cutting manual testing effort.
- Worked with security engineers to reproduce issues, verify product behaviour and improve detection accuracy.

Technical Skills

Security: MITRE ATT&CK, adversary emulation, detection validation, vulnerability assessment, web app testing

Tools: Wazuh, Suricata, Atomic Red Team, Burp Suite, Metasploit, Nmap, Wireshark, SQLMap, Gobuster, Hydra, Autopsy

Languages: Python, Bash, PowerShell, JavaScript, TypeScript, C, Java, SQL

Development: Next.js, React, Node.js, Express, Flask, PostgreSQL, Supabase, Playwright

Platforms: Kali Linux, Ubuntu/Debian, Windows, Docker, Git, GitHub Actions

Projects

Hacker-AI | *Next.js, tRPC, xterm.js, Better Auth, Inngest*

Private — demo on request

- AI-driven penetration testing platform with intelligent SOC monitoring for continuous threat response.
- Built an in-browser attack terminal (xterm.js), an Inngest job queue for long-running scans, and analyst RBAC.

Security Daily | *Node.js, GitHub Actions, RSS, Next.js*

modern.richujoseph.in/security-daily

- Scheduled pipeline that turns CVE, CISA, news and research feeds into a deduplicated daily threat-intel digest.

IoT Vulnerability Scanner | *Python, Flask, Shodan InternetDB, React*

GitHub

- Scans IoT devices for open ports, default credentials and exposed services, then maps findings to known CVEs.

AgroStack | *Next.js, ML forecasting*

GitHub

- ML crop-price forecasting with digital forward contracts for farmers; built in a team of five.

Achievements

- Most Innovative Agentic AI Solution** — Techashy '26 Hackathon, Apoorv 2026 (Hacker-AI).
- 1st Prize** — IEDC Cluster Hackathon (district level), IEDC Startup Summit 2026 (AgroStack).
- 1st Prize** — CYA Quest CTF, SJCET, Feb 2025 (team; web exploitation, cryptography, networking).
- Top 7 of 1,500+ participants** — Cinehack Hackathon, 2024.

Certifications

- TryHackMe Pre-Security Path (Feb 2026) — 90 rooms completed, 11 badges.
- Deloitte Cyber Job Simulation (Forage, 2026); Tata Cybersecurity Analyst Job Simulation (Forage, 2025).
- NPTEL — The Joy of Computing using Python, IIT Madras (Elite, 2025).

Leadership

- Guest Speaker & CTF Facilitator**, VJCET Vazhakulam (2025 – 2026) — organised and ran hands-on CTF events.
- College Ambassador**, RoomNumber404 (2025 – present) — security community outreach at SJCET.
- Department Coordinator**, national-level tech fest, SJCET (2025) — led technical execution and student teams.