

# Yashwanth Karuppusamy

✉ yashwanthkaruppusamy@gmail.com 📞 +91 9489400876 🌐 cyberwithyash.com in yashwanth98 📍 India

## Summary

---

Security Analyst with 2 years' experience in threat detection, incident response, and SIEM tools like Sentinel & Splunk. Familiar with SOAR, MITRE ATT&CK, and automation use cases.

## Education

---

**Swansea University** *Jan 2022 – Jan 2023*  
*MSc in Cybersecurity*

- **Coursework:** Cryptography & Network Security, Info sec Management, Pen Testing, Critical Systems

**Coimbatore Institute of Engineering and Technology** *Jun 2016 – Jul 2020*  
*B.E in computer science and engineering*

- **Coursework:** Software Engineering, Java, Computer Architecture, Design Analysis of Algorithms

## Skills

---

- **Threat Detection:** *Sentinel, Splunk, Defender, Darktrace, Akamai, FireEye, Sophos, Tenable, and Qualys.*
- **Compliance & Frameworks:** *MITRE ATT&CK Framework, ISO 27001, PCI DSS, and CASB.*
- **SOC Skills:** *KQL, MITRE Mapping, SOC Playbooks, MDR, SIEM Tuning, SLA, Elastic and QRadar.*
- **Soft Skills:** *Rapport Building, Excellent Communication, Adaptability and Team Collaboration.*

## Experience

---

**L2 SOC Analyst** *London, UK*  
*ITC Secure* *Oct 2024 – Apr 2025*

- Led 15+ targeted threat hunting engagements monthly, identifying root causes in 90% of post-incident reviews, which improved the precision of the SOC playbook and reduced repeat incidents.
- Used Qualys and Nessus for vulnerability assessments, reducing critical exposures by 15%.
- Triageed 80–110 daily alerts using Microsoft Sentinel, Defender, Darktrace and Qualys.
- Designed and delivered a SOC onboarding program that successfully transitioned 3 NOC engineers into Tier 1 SOC Analysts within 45 days.

**Security Analyst** *London, UK*  
*Hamilton Capital Holding* *Oct 2023 – Oct 2024*

- Created executive-level reports such as Threat Intelligence Reports, 4×4 briefings, and Risk assessment.
- Coordinated with 4+ Security vendors to align detection use cases with ISO 27001 standards and achieved 100% compliance in two successive internal audits.
- Tuned DLP and detection rules in Sentinel to reduce alert noise by 30%.
- Implemented monthly phishing simulations and awareness drives, reducing click rates from 22% to 6% within 3 months and improving team readiness scores by 40%.

## Projects

---

**A Game-Theoretic Approach to Robustness of Routing** *2022 - 2023*

- Enhanced network efficiency by 15% through implementing Nash equilibrium-based decision-making for node resilience.

**A Security Approach to Detect and Prevent ARP Spoofing using Active and Passive Techniques** *2019 - 2020*

- Enhanced network security by introducing dynamic MAC address rotation, reducing spoofing success rates by over 70