

# Rohit Kumar

rohitsharma1082001@gmail.com | 9027748842 | LinkedIn

## EXPERIENCE

### WIPRO LIMITED | SOC Analyst (L1)/ Cyber Security Analyst | Mar 2025 - Present | Pune, India

- Monitor and triage **40–60 security alerts per shift** using **Microsoft Sentinel** and **Defender XDR**.
- Investigate **300+ alerts/month** including malware, phishing, brute-force, and suspicious sign-ins.
- Handle **20+ confirmed incidents**, performing initial incident response, containment, and escalation.
- Execute **advanced hunting queries (KQL)** across endpoint, identity, email, and cloud logs, improving investigation accuracy by **25%**.
- Reduce false positives by **~20%** and maintain **100% SLA/SOP compliance**.

### Newfangled Vision Pvt Ltd | React Developer Nov 2024 - Mar 2025 | Pune, India

- Optimized React components using profiling tools, leading to a measurable **30% improvement** in UI performance and enhanced user experience across all user touchpoints.
- Developed and maintained **20+ reusable React components** within the first year, accelerating feature development cycles and improving code consistency across the application.

## PROJECTS

### TryHackMe – Labs & Rooms

- Completed **TryHackMe labs and rooms** focused on **SOC operations, threat detection, and attack techniques**.
- Hands-on practice with **SIEM concepts, log analysis, malware basics, phishing analysis, networking, and Windows security**.
- Strengthened **blue team operations**, understanding attacker behavior and defensive security techniques.

### Food Villa | React.js, JavaScript, Redux, Swiggy API | GitHub | Live

- Built a dynamic food discovery web application with **React.js** and third-party API integration.
- Implemented **cart functionality, live updates, search**, and routing using React Router.
- Applied **Redux state management** and wrote **unit tests** using Jest and React Testing Library.

### StreamHub | GitHub

- Developed an interactive video streaming platform using **React.js** and YouTube APIs.
- Optimized search performance using **debouncing and caching**, reducing redundant API calls.
- Implemented **live comment streaming**, improving real-time user engagement.

## EDUCATION

**Bachelor of Technology in Computer Science & Engineering**  
**ABES Engineering College**  
Nov 2021 – Jul 2024 | Ghaziabad, India

## LINKS

LinkedIn:// **RohitKumar**

Github:// **Rohit-108**

TryHackMe:// **rohit1082001**

## SKILLS

### PROGRAMMING

- Python • C++ • PowerShell • KQL  
(Kusto Query Language)

### SIEM / EDR / PLATFORMS

- Sentinel (SIEM & SOAR) • Splunk
- Microsoft Defender XDR • Wireshark
- Kali Linux • Azure Active Directory / Entra ID

### Security Operation & Domains

- SOC Operations (L1/L2) • Incident Detection & Response • Threat Intelligence & IOC Analysis • Endpoint & Identity Security • Phishing & Malware Analysis • Alert Triage & False Positive Reduction

### Networking & Fundamentals

- TCP/IP, DNS, DHCP, HTTP/HTTPS
- OSI Model • MITRE ATT&CK

## ACHIEVEMENTS

- Completed 30+ TryHackMe labs and rooms, gaining hands-on experience in SOC operations, SIEM analysis, malware detection, networking, and Windows security.
- Actively handled high-volume SOC alerts while maintaining investigation accuracy and SLA compliance.

## CERTIFICATIONS

- **AWS Cloud Practitioner**
- **Microsoft Security, Compliance, and Identity Fundamentals (SC-900)**
- **Microsoft Azure Security Engineer (AZ-500)**
- **Microsoft Security Operations Analyst (SC-200)**