

# SYED RAYAN

Bengaluru, Karnataka, India

+91 7892312126 | [syedrayan2k5@gmail.com](mailto:syedrayan2k5@gmail.com)

[linkedin.com/in/syed-rayan-profile](https://linkedin.com/in/syed-rayan-profile) | [github.com/syedrayan5](https://github.com/syedrayan5)

## Professional Summary

Cybersecurity Analyst skilled in SOC operations with hands-on experience in SIEM tools, log analysis, and threat detection. Committed to securing digital infrastructure and responding to cyber threats efficiently.

## Education

**HKBK Degree College, Bengaluru, India**

**2022-2025**

*Bachelor of Computer Applications*

CGPA: 8.7

## Technical Skills

- **Core Skills:** SOC Operations, Incident Response, Threat Detection & Analysis, Vulnerability Assessment, Network Security
- **Tools & Technologies:** SIEM (Splunk, QRadar, Sentinel), EDR (CrowdStrike, MS Defender), IDS/IPS (Snort, Suricata), VirusTotal
- **Soft Skills:** Analytical Thinking, Problem-Solving, Communication, Continuous Learning

## Projects

**Windows Failed Login Detection using IBM QRadar** | [Github](#)

- Configured QRadar to receive Windows log and created a detection rule for multiple failed login attempts
- Successfully triggered and visualized the alert in QRadar's Log Activity using synthetic events

**Brute Force Attack Detection using Splunk** | [Github](#)

- Ingested Windows logs into Splunk via Universal Forwarder and parsed Events to detect brute force attempts
- Built dashboards and configured real-time alerts for failed login patterns

**Suspicious Login Detection using ELK Stack + Wazuh** | [Github](#)

- Deployed ELK Stack with Wazuh and integrated a Windows VM to collect authentication logs
- Configured Wazuh rules to detect suspicious login activity and visualized events in Kibana

## Experience

**Cybersecurity Analyst Intern**

**Dec 2024 – Feb 2025**

*CodTech IT Solutions*

*Remote*

- Assisted in real-time log monitoring and performed initial triage of security alerts in a simulated SOC environment
- Analyzed phishing emails and escalated potential threats following incident response protocols
- Delivered an internal awareness session on phishing detection, improving team understanding of social engineering attacks

**Cybersecurity Analyst Intern**

**Jan 2025 – Feb 2025**

*CodeAlpha*

*Remote*

- Conducted secure code reviews to identify and document vulnerabilities in Python-based applications
- Developed a basic network sniffer in Python to analyze and detect malicious traffic patterns
- Published internship deliverables as public GitHub repositories demonstrating hands-on security skills

## Certifications

- Google Cybersecurity Certificate
- IBM Cybersecurity & Penetration Testing Certification
- EC-Council Vulnerability Assessment & Cloud Security Certification
- Ethical Hacking Certification (Internshala + NSDC)
- AI for Cybersecurity (Simplilearn + Udemy)

## Achievements / Extracurricular

- Secured top 3.25% rank among 4 lakh candidates in All India NCAT 2025
- Completed Cybersecurity Job Simulations with Tata, Mastercard, PwC, Deloitte, and AIG via Forage
- Contributed to Open-source security projects on GitHub
- Active member of NSS and national awareness campaigns