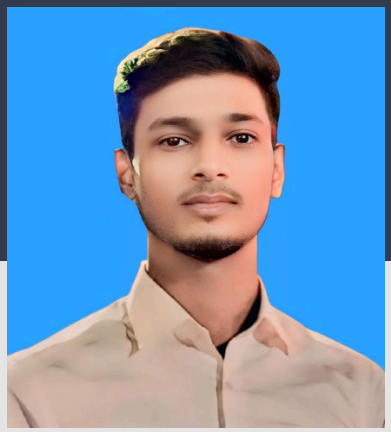

SURAJ MAURYA

SOC ANALYST

CONTACT

+91 8577978866

mauryasuraj638@gmail.com

Lucknow

SKILLS

- **SIEM** (SPLUNK, QRADAR)
- **IDS/IPS** (FAIL2BAN, SNORT)
- **XDR** (WAZUH)
- **NETWORKING** (OSI MODEL , TCP/IP , DNS ,DHCP ,HTTP/HTTPS, SSL , Firewall)
- **LINUX , UBUNTU**
- **PHISHING ANALYSIS (ANYRUN)**
- **MALWARE ANALYSIS**
- **VULNERABILITY ASSESSMENT** (BURPSUIT ZAPROXY NESSUS OPENVAS)
- **NETWORK TRAFFIC ANALYSIS** (WIRESHARK)

KEY ACHIVEMENT

- **Network Downtime Reduction**
- **Enhanced Response Efficiency**
- **System Security Enhancement**
- **Brute Force Defense**

LANGUAGES

- ENGLISH
- HINDI

PROFILE

I am a dedicated and passionate individual currently pursuing a B.Tech in Computer Science and Engineering. With expertise in cybersecurity tools and techniques, I have hands-on experience as a SOC Analyst intern. My projects involved utilizing Fail2Ban, Wazuh, and Snort for enhancing security protocols and threat monitoring. My goal is to make a meaningful impact in the field of cybersecurit

WORK EXPERIENCE

DURBHASI GURUKULAM

SOC Analyst INTERNSHIP — 08/2024 - 02/2025

- A Security Operations Center (SOC) Analyst internship is a hands-on opportunity to gain experience in cybersecurity by monitoring, detecting, and responding to security threats. Interns work with security tools like SIEMs, IDS/IPS, and firewalls to analyze logs, investigate incidents, and support the organization's cybersecurity posture. This role is ideal for individuals looking to develop skills in threat analysis, incident response, and network security while working in a fast-paced, teamoriented environment. .

EDUCATION

Bachelor of Technology

2021 - 2025

Dr. A. P. J. Abdul Kalam Technical University, Lucknow

CGPA: 6.8

PROJECT

Fail2ban

A project focused on enhancing security using Fail2Ban.

- Created custom Fail2Ban filters for Apache, Nginx, or MySQL.
- Monitored and reported incidents using Fail2Ban.
- Implemented rate limiting to prevent abuse.
- Defended against SSH brute force attacks.
- Protected web applications from SQL injection and XSS

WAZUH Security Monitoring Project (XDR)

A project involving security monitoring and incident response using Wazuh.

- Implemented Wazuh for log collection, monitoring, and threat detection across multiple systems
- Configured rules, alerts, and custom dashboards for real-time incident monitoring
- Configured rules, alerts, and custom dashboards for real-time incident monitoring
- Conducted vulnerability assessments and compliance checks

SNORT

A project aimed at enhancing network security with Snort.

- Created custom Snort rules
- Monitored malicious DNS traffic
- Integrated Snort with SIEM systems

CERTIFICATION

- CISCO CYBERSECURITY SPECIALIST (CCS)
- SOC ANALYST INTERSHIP BY DURBHASI GURUKULAM