

# NATTO MUNI CHAKMA

CybersecurityAnalyst | SOC Operations | SIEM & Incident Response

## CONTACT

Visakhapatnam, India  
Open to Relocation / Remote  
+91 9121691958  
nattochakma29@gmail.com  
LinkedIn: bit.ly/4p8CCAm  
GitHub: github.com/NATTOMR

## PROFESSIONAL SUMMARY

Cybersecurity-focused SOC Analyst with hands-on experience in SIEM monitoring, log analysis, threat detection, and vulnerability assessment across Windows and Linux environments. Strong understanding of authentication monitoring, brute-force detection, and incident response workflows.

## PROFESSIONAL EXPERIENCE

### Junior SOC Analyst Intern | LAUNCHED (Remote)

Apr 2025 – May 2025

- Monitored and analyzed security alerts using Splunk SIEM.
- Investigated suspicious login attempts and abnormal network behavior.
- Performed log analysis on Windows and Linux systems. Cybersecurity Intern |

### Elevats Labs (Cybersecurity Intern) - Remote

Jan 2026 – Apr 2026

- Conducted web application vulnerability assessments.
- Performed API security and authorization testing.
- Documented findings and recommended remediation strategies.

## PROJECT EXPERIENCE

- Final Year Project – Hybrid Android Malware Detection System
- Designed hybrid detection model combining static analysis and ML.
- Performed APK reverse engineering to extract permissions and API calls.
- Trained ML model for malware classification and evaluated performance metrics.
- SOC Homelab – SIEM Deployment & Attack Simulation
- Implemented centralized log collection using Splunk.
- Simulated SSH brute-force attacks and created alert dashboards.
- Linux SSH Attack Detection
- Monitored authentication logs for suspicious patterns.
- Generated structured incident reports.

## CORE SKILLS

- SIEM Monitoring (Splunk)
- Incident Response
- Threat Detection
- Log Analysis
- Event Correlation
- Vulnerability Assessment
- Brute-Force Detection
- Windows & Linux Security

## TECHNICAL TOOLS

- Splunk (SPL)
- Wazuh (SIEM)
- VirusTotal (Threat Intelligence Analysis)
- Wireshark
- Suricata
- Nmap
- Apktool / JADX
- Python (Scikit-learn)
- Bash, PowerShell, SQL

## EDUCATION

B.Tech – Computer Science & Engineering  
Andhra University - 2022 – 2026

## EXTRA CURRICULAR ACTIVITIES

- ICCR Scholar – Indian Council for Cultural Relations
- Cybersecurity Hackathon Participant
- Indian Navy Half Marathon – Top 100 / 1400 & 10KM Top 10
- Volunteer – University & Department Events
- Department Day Badminton Winner

## CERTIFICATIONS

- Google Cybersecurity Professional Certificate(2025)
- Ethical Hacking & Cybersecurity – NPTEL(2025)