MOHAMED IBRAHIM H

+91 8015562312 | ibrahim.cybrx@gmail.com | LinkedIn | GitHub | Ramanathapuram

SUMMARY

Cybersecurity student with hands-on SOC internship experience in SIEM monitoring, log analysis, and threat detection using Splunk, Wazuh, and Wireshark. Developed security automation projects including CTI pipelines, ML-based alert triage, and Zero Trust network simulation. Passionate about Blue Team operations and real-time threat monitoring.

KEY SKILLS

- Security Monitoring & Incident Response
- Splunk (SIEM) & Log Analysis
- Threat Intelligence (AlienVault OTX, AbuseIPDB, URLhaus)
- Network Security & Packet Analysis (Wireshark, Nmap)
- Zero Trust Architecture (NIST 800-207)

INTERNSHIP EXPERIENCE

SOC Analyst Intern **01/2026 - 04/2026**

The Mind IT | Hybrid

- Monitored and analyzed security events, alerts, and logs using **Splunk and Wazuh** to identify potential threats.
- Investigated security alerts and suspicious activities to support **incident response and threat detection**.
- Performed log analysis and security monitoring as part of daily **SOC operations**, contributing to the identification of suspicious activity.

PROJECTS

CTI Automation Platform | Python, Splunk REST API, AlienVault OTX, AbuseIPDB, URLhaus

- Engineered an automated **IOC collection pipeline** integrating AlienVault OTX, AbuseIPDB, and URLhaus threat feeds using Python REST APIs.
- Developed a **Splunk correlation engine** via REST API to match live IOCs against firewall and proxy logs, with a threat intelligence dashboard and automated severity classification (Critical/High/Medium/Low).

AI-Powered SOC Alert Triage System | Python, scikit-learn, Random Forest, Splunk

- Trained a **Random Forest classifier** on 2,000 labeled SOC alerts, achieving 98.5% test accuracy and ROC-AUC of 0.99.
- Built a real-time alert triage engine to classify **true vs false positives** with confidence scoring and automatically escalate Critical alerts to the Tier 2 queue.

Zero Trust Network Simulation Lab | pfSense, Wazuh, VirtualBox, Python, NIST SP 800-207

- Designed a four-zone **micro-segmented network** (SOC/DEV/MGMT/GUEST) based on NIST SP 800-207, using pfSense with 13 custom rules enforcing a default-deny policy.
- Built a Python-based **Zero Trust Policy Engine** using device trust, MFA, role, IP, and time-based controls; integrated Wazuh SIEM with 6 MITRE ATT&CK-mapped detection rules.

EDUCATION

Paavai Engineering College **11/2022 - 05/2026**

Bachelor of Engineering (B.E) in Cyber Security

CERTIFICATIONS

- EC-Council Certified SOC Analyst (CSA)
- EC-Council Ethical Hacking Essentials (EHE)
- Splunk Core Certified User
- Cisco Certified CyberOps Associate

ACHIEVEMENTS & ACTIVITIES

- Ranked among the **Top 5%** on TryHackMe - completed 40+ rooms covering web security, Linux privilege escalation, and network exploitation.
- Delivered a technical seminar on AI-Powered Threat Detection in SOC to 150+ students at the college tech symposium, covering ML-based alert triage and real-world detection workflows.