MOHAMED IBRAHIM H

+91 8015562312 | ibrahim.cybrx@gmail.com | Chennai, India | LinkedIn | GitHub | Portfolio

SUMMARY

Cybersecurity graduate and EC-Council Certified SOC Analyst (CSA) with SOC internship experience in SIEM monitoring, alert triage, log correlation, and incident response using Splunk, Wazuh, and Wireshark. Engineered automated CTI pipelines, ML alert triage engines (98.5% lab accuracy), and NIST SP 800-207 Zero Trust labs for Blue Team defense.

TECHNICAL SKILLS

SIEM & Monitoring: Splunk (SPL), Wazuh, Microsoft Sentinel, alert triage, log correlation, dashboards
Detection & Response: Incident Response, Phishing Analysis, MITRE ATT&CK, IOC analysis, Alert Tuning, ServiceNow
Threat Intelligence: AlienVault OTX, AbuseIPDB, URLhaus, MISP, CTI automation
Network & Endpoint: Wireshark, pfSense, Suricata, EDR/XDR, Defender, Active Directory, Sysmon, TCP/IP, DNS
Programming & Infra: Python (REST APIs, scikit-learn), SPL, Bash, PowerShell, Linux, Docker
Frameworks: MITRE ATT&CK, NIST SP 800-207, Zero Trust Architecture

EXPERIENCE

SOC Analyst Intern **01/2026 – 04/2026**
The Mind IT *Hybrid*

- Triaged 40+ daily security alerts in Splunk and Wazuh across authentication, endpoint, and network logs, classifying true/false positives and escalating 15+ confirmed incidents to senior analysts within 15-minute SLA windows with supporting evidence.
- Investigated 30+ weekly anomalies—including failed-login bursts, suspicious outbound traffic, and port-scan activity—using SPL correlation searches and threat intelligence validation (AbuseIPDB, AlienVault OTX), documenting 20+ end-to-end incident timelines in tickets.
- Analyzed 25+ suspicious packet captures in Wireshark to confirm malicious behavior and flagged 8+ noisy detection rules for tuning, reducing recurring false-positive alert volume by ∼25% and improving alert quality.

PROJECTS

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

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

AI-Powered SOC Alert Triage System GitHub Repo
Python, scikit-learn, Random Forest

- Built a Random Forest alert classifier in Python (scikit-learn) on a 2,000-alert synthetic/lab dataset (severity, source IP reputation, event type, frequency), achieving 98.5% held-out test accuracy and 0.99 ROC-AUC.
- Implemented a triage engine that assigns confidence scores to each alert, automatically escalating Critical high-confidence alerts to a Tier 2 queue while auto-closing low-risk false positives.

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

- Designed a four-zone micro-segmented network (SOC/DEV/MGMT/GUEST) aligned with NIST SP 800-207 using pfSense with 13 custom firewall rules enforcing a default-deny policy.
- Built a Python Zero Trust policy engine (device trust, MFA, role, source IP, time window) paired with a Wazuh SIEM monitor raising alerts across 6 MITRE ATT&CK-mapped detections.

EDUCATION

Bachelor of Engineering (B.E) in Cyber Security **11/2022 – 05/2026**
Paavai Engineering College | CGPA: 7.5/10

- **Publication:** "Creating Tailored Detection and Prevention Mechanisms for Targeted Threats," *IJARIIT* (2025).
- **Coursework:** NPTEL – Software Project Management, IIT Kharagpur.

CERTIFICATIONS

- EC-Council Certified SOC Analyst (CSA) | Cisco Certified CyberOps Associate
- Splunk Core Certified User | EC-Council Ethical Hacking Essentials (EHE)
- Wazuh Ambassador – Certificate of Recognition (Open-Source SIEM/XDR Community)

ACHIEVEMENTS

- Ranked **Top 4%** globally on TryHackMe (Sapphire League); completed **60+ rooms** and SOC Simulator scenarios (100% true positive rate) covering log analysis, Linux privilege escalation, and network defense.
- Delivered a technical seminar on *AI-Powered Threat Detection in SOC* to 150+ students, covering ML-based alert triage and real-world detection workflows.