Jefrine Correya

SOC Analyst L1

+91 8113064878 | jefrincorreya@gmail.com | linkedin.com/in/jefrine07 | jefrincyberportfolio.com | Kochi, Kerala, India

PROFESSIONAL SUMMARY

Detail-oriented and highly skilled SOC Analyst with specialized expertise in cybersecurity and threat intelligence. Skilled in real-time monitoring, analysis, and effective response to security incidents using advanced tools and technologies. Proficient in threat detection, incident response, vulnerability analysis, and risk mitigation. Experienced with SIEM solutions and other monitoring platforms, ensuring swift detection and containment of potential threats. Strong communicator with a team-focused mindset, dedicated to continuous learning and remaining current on emerging cybersecurity threats, tools, and best practices in the security landscape.

TRAINING

- **02.2025 - 07.2025 CICSA (Certified IT Infrastructure and Cyber SOC Analyst, RedTeam kochi)**
  - Practical training in Security Operations Center (SOC) workflows
  - Worked with tools: Nmap, Burp Suite, Wireshark, Splunk, Metasploit
  - Skills: Threat detection, incident response, vulnerability assessment, network analysis
  - Hands-on exposure to real-time cyberattack scenarios and response techniques

EDUCATION

- **10.2021 - 08.2024 Bachelor of Computer Applications**
  Koshys Institute of Management Studies, Banglore North University, Karnataka, Banglore, India

SKILLS

- **Tools** - Splunk (SIEM Tool), Wireshark (Network Analysis), Burp suite (Web Application Security), Nmap, OSINT Tools, Metasploit, Nessus
- **SOC** - Incident Detection, Incident Response, Knowledge of Cyber Attacks
- **Networking** - Network Traffic Analysis, OSI model, Firewall, TCP/IP, Networking Protocols, IDS/IPS, VPN
- **Operating Systems** - Windows, Kali Linux, MacOS
- **Programming Languages** - HTML, CSS, Python, MySQL, Javascript
- **Machine Learning** - Scikit-learn ,Isolation Forest, Random Forest,
- **Soft Skills** - Problem-Solving, Teamwork, Communication skills, Continuous Learning
- **Languages** - Malayalam, English, Kannada

PROJECT

- **> AI-Powered SOC Threat Detection Assistant (CrewAI Agents)**
  Developed an AI-driven SOC automation system with four CrewAI agents to streamline threat detection and triage. Automated IP extraction from logs, AbuseIPDB enrichment, GeoIP lookups, and structured investigation reporting—reducing manual effort and accelerating SOC response.
  Technologies: Python, CrewAI, AbuseIPDB API, GeoIP Services, Regex.
- **> URL Phishing Detector**
  Built a web-based phishing detection tool using Flask, allowing users to submit URLs for real-time risk analysis. Combined lexical feature analysis with Google Safe Browsing API to identify and flag malicious or phishing links.
  Technologies: Python (Flask), Google Safe Browsing API, HTML, CSS, JavaScript.
- **> ML Threat Monitor**
  Created an ML-driven monitoring tool to detect anomalies and threats in real-time using machine learning. Analyzed logs and traffic to identify suspicious behavior, providing early warnings for proactive incident response.
  Technologies: Nmap, HTML, TailwindCSS, Python (Flask), Scikit-learn(ML).

CERTIFICATIONS

- **09.2025 Certified SOC Analyst v1**
  EC Council
- **07.2025 IT Infrastructure and SOC Analyst**
  Redteam Hacker Academy