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
- **Soft Skills** - Problem-Solving, Teamwork, Communication skills, Continuous Learning
- **Languages** - Malayalam, English, Kannada

PROJECT

- **> Web Vulnerability Scanner**
  Created a Flask-based tool to scan websites for open ports and vulnerabilities using Nmap. It features a user-friendly interface and provides real-time scan results for proactive security checks. Designed to simulate real-world reconnaissance techniques used in penetration testing.
  Technologies: Python (Flask), Nmap, HTML, TailwindCSS.
- **> AI Threat Monitor**
  Created an AI-driven monitoring tool to detect anomalies and potential threats in real-time using machine learning techniques. The system analyzes network traffic and security logs to identify suspicious behavior, providing early warnings for proactive incident response. Designed to emulate real-world SOC detection workflows and improve threat visibility through intelligent alerting.
  Technologies: Python (Flask), Scikit-learn, Pandas, JSON, HTML, TailwindCSS, JavaScript

CERTIFICATIONS

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