Gopalakrishnan Palpandi

+91 9342336959 | messagetogkr@gmail.com | linkedin.com/in/Gopalakrishnan_Palpandi | github.com/mactavishtony

Professional Summary

Detail-oriented SOC Analyst with hands-on experience in security monitoring, log analysis, and incident response within simulated enterprise environments. Proficient in SIEM platforms, IDS monitoring, and threat detection aligned with the MITRE ATT&CK framework. Strong foundation in Linux, networking fundamentals, and blue team operations with a focus on safeguarding organizational assets.

Education

Sri Ramakrishna College of Arts and Science — Coimbatore
Bachelor of Science in Computer Science — *June 2022 – May 2025*

PSG Sarvajana — Coimbatore
Higher Secondary Education — *July 2020 – May 2022*

Certifications

Security Blue Team Pathway — Security Blue Team
Hands-on SOC and Defensive Security Training — *2025*

Experience

Graduate Trainee — July 2025 – Present
Microland Limited — *Remote*

- Supported monitoring of system alerts, logs, and service tickets in an enterprise environment.
- Assisted with incident handling, escalation workflows, and basic root cause analysis.
- Gained exposure to IT operations, security awareness, and SOC-related processes.

Founder and Security-Focused Front-End Developer — September 2024 – July 2025
Webz Wave Solutions — *Remote*

- Led a team of 8 members delivering secure web applications with an emphasis on data protection.
- Applied OWASP secure coding practices and basic access control mechanisms.
- Reviewed application logs to identify anomalies and potential security issues.

Projects

SOC Home Lab – Blue Team Operations | *Wazuh, ELK Stack, pfSense, VMware* — December 2024

- Built a virtual enterprise SOC environment using VMware.
- Configured Wazuh agents for log collection, FIM, and alerting.
- Monitored IDS alerts and correlated events using SIEM dashboards.
- Mapped threats to the MITRE ATT&CK framework and documented response actions.

High-Security Video Analytics Framework | *Python, OpenCV, AI* — October 2024

- Developed a real-time surveillance analytics system for intrusion detection.
- Implemented anomaly detection and unauthorized access recognition.
- Generated alerts based on suspicious motion and behavior patterns.

Technical Skills

SOC & Blue Team Skills: Security Monitoring, Log Analysis, Alert Triage, Incident Response, Threat Detection
SIEM & Security Tools: Wazuh, Security Onion, ELK Stack, Wireshark, pfSense
Frameworks: MITRE ATT&CK
Operating Systems: Linux (Ubuntu, Kali), Windows
Networking: TCP/IP, DNS, HTTP/S, Firewalls, IDS/IPS
Scripting: Python, Bash
Platforms: VMware, Google Cloud Platform

Declaration

I hereby declare that the above information is true and correct to the best of my knowledge.