ANUGRAH KIZHAKKE VEEDU

Bahrain | +91 8547743622 | anugrahkv07@gmail.com
linkedin.com/in/anugrah | github.com/Anugrahkv | Portfolio Website

PROFESSIONAL SUMMARY

Detail-oriented Cybersecurity professional with an MSc in Cyber Security and hands-on experience turning noisy environments into monitored, hardened, and audit-ready systems. Specialized in SOC operations, proficient in deploying full IDS pipelines (pfSense, Suricata, ELK Stack), executing threat analysis mapped to the MITRE ATT&CK framework, and developing automated triage tools. Seeking a SOC Analyst position to leverage strong infrastructure hardening, log analysis, and incident response capabilities to defend enterprise perimeters.

TECHNICAL SKILLS

Security Operations (SOC): Threat Hunting, Malware Analysis, Phishing Analysis, Log Analysis, Incident Response, Vulnerability Assessments, MITRE ATT&CK Mapping.
SIEM & Network Defense: ELK Stack (Elasticsearch, Logstash, Kibana), Next-Generation Firewalls (FortiGate, pfSense), Intrusion Detection Systems (Suricata, Snort), Splunk familiarity, VPNs, Wazuh.
Analysis Tools & Admin: Any.Run Sandbox, Wireshark, Linux Server Administration, Command-Line Interfaces (CLI).
Security Automation & Scripting: Python, Django, REST API Integration (VirusTotal, AbuseIPDB), JSON Parsing, OWASP Top 10 Mitigation.

PROFESSIONAL EXPERIENCE

Btrac Solutions | Kerala, India **July 2022 – March 2023**
Web Application Developer (Intern) – Security & Infrastructure Focus

- Supervised day-to-day operations, log consistency, and system patch levels across internal evaluation servers and **3** isolated client-facing production hosting nodes.
- Proactively identified and mitigated **OWASP Top 10 vulnerabilities** prior to production release cycles, contributing to measurable reductions in attack surface exposure.
- Collaborated with engineering teams to securely deploy patches across staging and production environments, maintaining critical web components using Python and the Django framework.
- Implemented secure cryptographic authentication protocols and database integrations to safeguard sensitive user data integrity for **1,000+** relational records.

KEY PROJECTS

Active SOC Home Lab & Threat Hunting Environment **July 2026**
Technologies: VirtualBox, SIEM Wazuh, Snort IDS, Kali Linux

- Architected a multi-subnet virtualized SOC environment utilizing VirtualBox, establishing isolated NAT and Host-Only networks to safely execute and monitor attack simulations.
- Deployed a centralized defense infrastructure featuring a Wazuh SIEM, integrating a Snort NIDS engine to ingest, parse, and analyze internal lab traffic.
- Engineered an attack-and-defend pipeline by configuring a Kali Linux adversary node to launch targeted activity against a Linux victim machine, validating SIEM detection and alert logic.

Advanced Malware Detonation & C2 Extraction | *Independent Project* **June 2026**
Technologies: Any.Run Sandbox, Suricata IDS, MITRE ATT&CK, OSINT

- Executed and analyzed weaponized malware payloads (Macro-enabled documents) within an isolated Any.Run cloud sandbox to map runtime execution graphs and process injection sequences.
- Extracted actionable Indicators of Compromise (IoCs), identifying external Command & Control (C2) IP infrastructure and spoofed user-agent beaconing behavior over HTTPS.
- Correlated network telemetry with Suricata IDS signatures and mapped adversary Tactics, Techniques, and Procedures (TTPs) directly to the MITRE ATT&CK framework.

SOC Automation & Enrichment Dashboard | *Independent Project* **June 2026**
Technologies: Python, Django, REST APIs (VirusTotal v3, AbuseIPDB), JSON

- Engineered a custom Tier 1 SOC triage dashboard to automate the enrichment of Indicators of Compromise (IOCs) and reduce manual alert fatigue.
- Developed intelligent backend auto-routing logic and integrated RESTful APIs to extract and parse complex JSON threat intelligence for network reputation and multi-engine malware telemetry.

- Conducted rigorous True Positive and True Negative validation simulations against live malware hashes (e.g., WannaCry) and active scanner IPs to verify engine accuracy.

Intrusion Detection & Threat Monitoring System (IDS) **September 2023 – September 2024**
Master's Project – Teesside University
Technologies: Ubuntu Server, pfSense, Suricata, ELK Stack

- Designed and deployed a production-simulating multi-layered IDS environment from scratch, integrating an open-source firewall, intrusion detection system, and real-time monitoring tools.
- Built a centralized SIEM pipeline using Elasticsearch, Logstash, and Kibana to aggregate multi-source security logs, reducing manual log review time by **30%**.
- Engineered **15+ custom detection rules** using Suricata, reducing false-positive alerts by **20%** while expanding defensive visibility against critical CVEs mapped to MITRE ATT&CK vectors.

TrippyGo – Secure Full-Stack Web Application **2023**
Bachelor's Project – Kannur University
Technologies: Python, Django, HTML, CSS, SQLite

- Engineered a full-stack application with a security-first approach, implementing robust cryptographic session management and strict input validation to systematically eliminate SQL injection and XSS vulnerabilities.
- Applied MVC architecture principles and developed automated maintenance scripts to ensure secure database handling with **zero deployment downtime**.

CERTIFICATIONS & TRAINING

Fortinet Certified Associate (FCA) | *Fortinet | ID: 9668149803AK* **June 2026**
Fortinet Certified Fundamentals (FCF) | *Fortinet | ID: 7103587775AK* **June 2026**
Mastercard Cybersecurity Job Simulation | *Forage* **June 2026**
Linux Fundamentals | *Hack The Box Academy* **June 2026**
Elastic Ecosystem & Technical Essentials | *Elastic | ID: LP1357* **June 2026**

Currently Enrolled Professional Development:
• **Certified Ethical Hacker (CEH)** | *Expected: October 2026*
• **Certified IT Infrastructure & Cyber SOC Analyst (CICSA)** | *Expected: October 2026*

EDUCATION

Teesside University | Middlesbrough, UK **2023 – 2024**
Master of Science in Cyber Security

Kannur University | Kerala, India **2020 – 2023**
Bachelor's Degree in Computer Application