ANUGRAH KIZHAKKE VEEDU

Kannur, Kerala, India | +91 8547743622 | anugrahkv07@gmail.com
Linkedin/anugrah | Github/Anugrah | Portfolio/anugrah

PROFESSIONAL SUMMARY

Cybersecurity professional with an MSc in Cyber Security and hands-on experience across SOC operations, security monitoring, threat hunting, vulnerability assessment, malware analysis, and web application security. Experienced in building and operating security labs using Wazuh, ELK Stack, Suricata, Snort, pfSense, and Linux, with practical exposure to SIEM alert investigation, IDS rule development, IOC enrichment, MITRE ATT&CK mapping, and incident triage. Strong scripting and automation skills using Python and REST APIs. Seeking SOC Analyst, Security Analyst, Junior Cybersecurity Analyst, or Blue Team roles.

TECHNICAL SKILLS

SOC & Security Operations: Security Monitoring, Alert Triage, Threat Hunting, Incident Response, IOC Analysis, Log Analysis, Phishing Analysis, Malware Analysis, MITRE ATT&CK, Threat Intelligence
SIEM, IDS/IPS & Network Security: Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, Suricata, Snort, pfSense, FortiGate, Network Traffic Analysis
Vulnerability Assessment & Web Security: Burp Suite, OWASP Top 10, Web Application Security Testing, Vulnerability Assessment, Secure Coding, Input Validation, Authentication & Session Security
Malware Analysis & Threat Intelligence: Any.Run, VirusTotal, AbuseIPDB, IOC Extraction, C2 Identification, Sandbox Analysis, OSINT
Systems & Tools: Linux/Ubuntu Server, Kali Linux, Wireshark, VirtualBox, Command Line, Git, JSON
Programming & Automation: Python, Django, REST APIs, JSON Parsing, Security Automation, Automated IOC Enrichment, Triage Scripting

PROFESSIONAL EXPERIENCE

Btrac Solutions **July 2022 – March 2023**
Web Application Developer Intern – Security & Infrastructure Focus

- Supported application and infrastructure operations across internal evaluation systems and **3 client-facing hosting nodes**, including monitoring, maintenance, security updates, and troubleshooting.
- Performed security-focused testing of web applications using OWASP Top 10 principles and Burp Suite techniques to identify common application vulnerabilities before deployment.
- Collaborated with development and infrastructure teams to deploy application updates and security patches across staging and production environments.
- Developed and maintained Python/Django components with emphasis on secure authentication, input validation, database security, and protection of sensitive application data.

CYBERSECURITY PROJECTS

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

- Built a segmented virtual SOC environment using VirtualBox with isolated NAT and Host-Only networks for controlled attack simulation and security monitoring.
- Deployed Wazuh as the central SIEM and integrated Snort IDS to collect, correlate, and investigate security events generated within the lab environment.
- Simulated attacker activity from Kali Linux against a Linux victim system and validated SIEM detection, alert generation, and investigation workflows.
- Practiced SOC workflows including event analysis, suspicious activity investigation, alert triage, and identification of potential indicators of compromise.

Advanced Malware Detonation & C2 Analysis **June 2026**
Any.Run, Suricata, MITRE ATT&CK, OSINT

- Analyzed malicious macro-enabled documents in an isolated Any.Run sandbox, examining process execution, network activity, and behavioral indicators.
- Extracted Indicators of Compromise (IOCs), including suspicious IP addresses, domains, user-agent activity, and Command-and-Control (C2) communication patterns.
- Correlated malware network activity with Suricata alerts and mapped observed attacker behaviors to relevant MITRE ATT&CK tactics and techniques.
- Documented findings as actionable threat intelligence for detection and incident investigation.

SOC Automation & IOC Enrichment Dashboard **June 2026**
Python, Django, VirusTotal API v3, AbuseIPDB API, REST, JSON

- Developed a Python/Django-based SOC triage dashboard to automate IOC enrichment and reduce repetitive manual investigation tasks.

- Integrated VirusTotal and AbuseIPDB REST APIs to retrieve malware intelligence, IP reputation, and multi-source threat information.
- Implemented backend processing and JSON parsing to automatically classify and enrich submitted indicators for analyst investigation.
- Validated the workflow using known malicious hashes and suspicious scanner IPs to test enrichment results and triage logic.

Intrusion Detection & Threat Monitoring System **September 2023 – September 2024**
Master's Project – Teesside University
Ubuntu Server, pfSense, Suricata, Elasticsearch, Logstash, Kibana

- Designed and deployed a layered network security environment integrating pfSense firewall, Suricata IDS, and the ELK Stack for centralized security monitoring.
- Built a centralized log pipeline using Elasticsearch, Logstash, and Kibana to collect, process, visualize, and investigate security events from multiple sources.
- Developed and tested **15+ custom Suricata detection rules** for network threats and security events, improving visibility into suspicious traffic.
- Reduced manual log review time by approximately **30%** through centralized security event collection and visualization.
- Investigated IDS alerts and correlated network events with relevant MITRE ATT&CK techniques and known vulnerability patterns.

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

- Developed a full-stack Django web application with security-focused authentication, input validation, database access controls, and session management.
- Applied secure development practices to mitigate common web vulnerabilities including SQL injection and Cross-Site Scripting (XSS).

CERTIFICATIONS & PROFESSIONAL TRAINING

Fortinet Certified Associate (FCA) **June 2026**
Fortinet | Credential ID: 9668149803AK
Fortinet Certified Fundamentals (FCF) **June 2026**
Fortinet | Credential ID: 7103587775AK
Elastic Ecosystem & Technical Essentials **June 2026**
Elastic | Credential ID: LP1357
Linux Fundamentals **June 2026**
Hack The Box Academy
Mastercard Cybersecurity Job Simulation **June 2026**
Forage
Currently Enrolled – Red Team Hacker Academy, Calicut:
Certified Ethical Hacker (CEH) | Expected October 2026
Certified IT Infrastructure & Cyber SOC Analyst (CICSA) | Expected October 2026

EDUCATION

Teesside University **2023 – 2024**
MSc Cyber Security Middlesbrough, UK
Kannur University **2020 – 2023**
Bachelor of Computer Applications Kerala, India