DHANANJAY KRISHNAN K P

Cybersecurity Analyst

+91-8089983975 kp.dhananjaykrishna@gmail.com Linkedin GitHub

PROFILE SUMMARY

Cybersecurity professional with hands-on experience in phishing detection, domain takedown operations, threat intelligence, and log analysis. Skilled in SIEM tools, network monitoring, and working with CTI and OSINT platforms. Strong understanding of security operations, incident response, and vulnerability assessment. Detail-oriented team player with a proactive approach to solving security challenges.

EDUCATION

Red Team Hacker Academy **August 2024 - February 2025**
Certified IT infrastructure and Cyber SOC Analyst *Kozhikode, Kerala*

School of Computer Sciences, Mahatma Gandhi University **July 2022 - August 2024**
Master of Science in Computer Science *Kottayam, Kerala*

EXPERIENCE

TIKAJ TECHNOLOGIES PVT LTD **February 2025 – Present**
SOC Analyst L1 *Lucknow, Remote*

- Monitored and analyzed security alerts to detect and mitigate potential threats in real-time using Hunto AI.
- Performed initial triage, assessed severity levels, and escalated critical incidents for further investigation.
- Created, updated, and managed incident tickets with complete documentation and timely follow-ups.
- Delivered Anti-Phishing Services to protect clients from deceptive phishing attacks and related cyber threats.
- Brand Monitoring Services, tracking and defending client brand reputation across the surface, deep, and dark web.
- Handled over 5,000+ incidents weekly, including detections and takedowns of phishing sites, fraudulent web pages, malicious applications, and impersonated social profiles.
- Collaborated with leading clients across e-commerce, manufacturing, and finance sectors to protect their digital assets and maintain brand integrity.

PROJECTS

PhishRecon – Phishing & Threat Intelligence CLI Tool | *Python, VirusTotal API, OSINT Tools* **June 2025**

- Built a CLI-based threat intelligence tool to identify phishing and suspicious domains.
- Integrated multiple OSINT tools for subdomain enumeration, IP/email discovery, and threat enrichment.
- Automated real-time scanning and VirusTotal lookups to flag malicious or suspicious indicators.
- Implemented automated threat scoring based on HTTP status codes and VirusTotal malicious indicators.

Real-Time Threat Detection and Log Correlation Using Splunk | *Splunk* **January 2025**

- Developed a centralized log correlation system for monitoring security incidents.
- Created custom dashboards, alerts, and automated scripts for threat detection and mitigation.
- Implemented threat intelligence feeds to enhance visibility into advanced persistent threats (APT).

TECHNICAL & PROFESSIONAL SKILLS

Programming Languages: Python, SQL, Bash

Security Tools: Splunk, QRadar, SOAR, IDS/IPS, EDR, Nessus, Wireshark, Burp Suite, Wazuh, Snort, Hunto AI

Operating Systems: Kali Linux, Ubuntu, Windows

Networking: TCP/IP, DNS, Firewalls, VPNs, OSI Model

Frameworks and Standards: MITRE ATT&CK, NIST, ISO 27001, PCI-DSS

Soft Skills: Problem-Solving & Analysis, Attention to Detail, Communication & Teamwork, Critical Thinking, Adaptability & Continuous Learning, Time Management, Report Writing & Documentation.

CERTIFICATIONS & QUALIFICATIONS

CSA (Certified SOC Analyst)
August 2024 - February 2025

EC-Council *ECC0875134296*

- Gained hands-on expertise in monitoring and responding to security incidents, analyzing logs, and using SIEM tools for threat detection and mitigation in a SOC environment.

Certified IT Infrastructure and Cyber SOC Analyst (CICSA v3)
August 2024 - February 2025

RedTeam Hacker Academy *RTXSTU1682011875*

- Comprehensive training on IT infrastructure security, real-time threat hunting, incident response, malware analysis, and SOC operations with practical lab sessions using industry-grade tools.

Cybersecurity Analyst Certifications
December 2024 - January 2025

IBM, Cisco, Microsoft, Tata Group, Reliance

- Completed multiple certifications across key cybersecurity areas, including network security, threat detection, IAM, cloud security, SOC operations, and compliance frameworks.

UGC-NET Qualified for PHD (2024)
December 2024

Computer Science & Applications *24D/03/045153*

- Qualified for the National Eligibility Test (NET) for PhD in Computer Science, demonstrating foundational and research-level understanding in areas like algorithms, data structures, operating systems, and cybersecurity principles.