Dhananjay Krishnan K P

Phone: +91-8089983975 | offcl.dhananjaykrishna@gmail.com | LinkedIn | Portfolio

Professional Summary

Certified SOC Analyst (EC-Council CSA) with 1+ year of hands-on experience in threat detection, phishing investigation, and incident response across enterprise SOC environments. Proven track record handling 5,000+ weekly security incidents involving phishing sites, malicious domains, fraudulent applications, and brand impersonation campaigns. Experienced with SIEM, NDR, EDR, and XDR platforms, MITRE ATT&CK mapping, OSINT analysis, and coordinating domain takedowns with hosting providers and abuse teams. Seeking to apply deep operational expertise in a cybersecurity analyst role.

Professional Experience

Cybersecurity Analyst Trainee (Internship) September 2025 – February 2026
Tracelay Networks Pvt Ltd *Bangalore, India*

- Monitored and triaged security alerts across SIEM, NDR, EDR, and XDR platforms including ExtraHop NDR, TrendMicro Vision One XDR, Cybereason EDR, CyberArk IAM, IBM X-Force, and Sumo Logic NG-SIEM.
- Investigated security incidents and mapped adversary behaviour to MITRE ATT&CK tactics, techniques, and procedures (TTPs) to improve root cause analysis accuracy and incident classification.
- Assisted in building AI-assisted triage workflows using n8n (rule-based and agent-driven) to correlate multi-platform alerts, reduce false positives, and accelerate analyst response times.
- Produced detailed incident reports and forensic documentation with root cause analysis and remediation recommendations, delivered to senior analysts and stakeholders.
- Participated in threat hunting exercises to proactively identify indicators of compromise (IOCs) and suspicious lateral movement across enterprise infrastructure.

SOC Analyst February 2025 – Present
Tikaj Technologies | Hunto AI *Lucknow, India (Remote)*

- Handled 5,000+ weekly security incidents covering phishing site detections, fraudulent web pages, malicious mobile applications, and brand impersonation across social media platforms.
- Investigated phishing infrastructure using OSINT techniques to map malicious domains, IP addresses, hosting providers, and related threat actor infrastructure.
- Coordinated takedown requests for phishing domains, fraudulent assets, and impersonation profiles with hosting providers, registrars, and platform abuse teams, achieving rapid deactivation of malicious content.
- Executed Brand Monitoring operations tracking client brand reputation across surface web, deep web, and dark web environments for clients in e-commerce, manufacturing, and finance sectors.
- Performed alert triage, initial incident investigation, and documented findings with remediation actions in security ticketing systems, maintaining clear audit trails for all cases.
- Mentored junior analysts on triage procedures, alert escalation workflows, and OSINT investigation techniques to improve overall team effectiveness.

Education

Mahatma Gandhi University (MGU), Kottayam Kottayam, Kerala, India
Master of Computer Science *July 2022 – August 2024*

RedTeam Hacker Academy Calicut, Kerala, India
Certified IT Infrastructure and SOC Analyst *August 2024 – February 2025*

Security Projects

PhishRecon – Phishing Infrastructure Reconnaissance Tool
Personal Project | Python, VirusTotal API, OSINT

- Built a Python-based CLI tool to automate reconnaissance on suspicious domains, correlating data from VirusTotal API, WHOIS records, DNS lookups, and OSINT sources to map phishing infrastructure.
- Implemented automated reputation scoring and IOC extraction for domains and associated IP addresses, enabling faster identification of malicious hosting patterns.
- Reduced manual investigation time for phishing domain analysis by automating intelligence gathering workflows previously performed across multiple disparate tools.

Technical Skills

SIEM & Monitoring: Sumo Logic NG-SIEM, IBM X-Force, Alert Triage, Log Analysis, IOC Detection
Endpoint & Network Security: ExtraHop NDR, TrendMicro Vision One XDR, Cybereason EDR, CyberArk IAM, IDS/IPS
Threat Intelligence & OSINT: VirusTotal, WHOIS, DNS Analysis, Brand Monitoring, Dark Web Monitoring, Phishing Detection & Takedown, Malicious Domain Analysis
Incident Response: MITRE ATT&CK Mapping, Root Cause Analysis, Forensic Documentation, Ticketing Systems, Abuse Team Coordination
Security Frameworks: MITRE ATT&CK, Cyber Kill Chain, NIST CSF, Incident Response Lifecycle
Automation & Scripting: Python, Bash, n8n (Workflow Automation)

Certifications & Achievements

EC-Council Certified SOC Analyst (CSA) – Professional certification in SOC operations, threat detection, and incident response
Certified IT Infrastructure and SOC Analyst – Comprehensive SOC and IT infrastructure security training, RedTeam Hacker Academy
UGC NET PhD Qualified – National eligibility for doctoral research in Computer Science