Dhananjay Krishnan K P

+91-8089983975 | offcl.dhananjaykrishna@gmail.com | linkedin.com/in/dhananjay-krishna-k-p |
portfolio.dhananjaykrishnakp.com | Bengaluru, India (Open to Relocation)

Professional Summary

EC-Council Certified SOC Analyst with 1+ year of hands-on experience in security monitoring, threat detection, and incident response within enterprise SOC environments. Demonstrates proven ability to implement procedural changes, maintain security documentation, and analyze security incidents end-to-end. Experienced across SIEM, NDR, EDR, and XDR platforms with practical skills in MITRE ATT&CK mapping, OSINT investigation, risk analysis, and coordinating remediation with internal and external stakeholders. Adept at learning and applying organizational security standards and regulatory requirements, and at supporting senior analysts on complex analysis and response workflows.

Professional Experience

SOC Analyst February 2025 – March 2026
Tikaj Technologies | Hunto AI *Remote, India*

- Monitor and triage 5,000+ weekly security incidents covering phishing detections, fraudulent web pages, malicious mobile applications, and brand impersonation – maintaining clear audit trails and security documentation for all cases.
- Implement procedural changes to triage workflows, improving incident classification accuracy and analyst response consistency across a high-volume alert environment.
- Research and analyze attempted external compromise efforts using OSINT techniques to map malicious domains, IP addresses, hosting providers, and threat actor infrastructure.
- Develop and apply mitigation strategies by coordinating takedown requests with hosting providers, domain registrars, and platform abuse teams, achieving rapid deactivation of malicious assets.
- Create and maintain security documentation including incident reports, investigation logs, and remediation records in ticketing systems, ensuring compliance with audit and reporting standards.
- Assist senior analysts during escalated investigations and transitions, contributing to brand monitoring operations across e-commerce, manufacturing, and finance sectors.

Cybersecurity Analyst Trainee (Part-time Training Program) September 2025 – February 2026
Tracelay Networks Pvt Ltd *Remote, Bangalore, India*

- Took a structured part-time internship to gain deeper exposure.
- Monitored and triaged security alerts across enterprise SIEM, NDR, EDR, and XDR platforms including Sumo Logic NG-SIEM, IBM X-Force, ExtraHop NDR, TrendMicro Vision One XDR, Cybereason EDR, and CyberArk IAM.
- Investigated security incidents and mapped adversary behaviour to MITRE ATT&CK TTPs to improve root cause analysis accuracy and incident classification.
- Co-developed AI-assisted triage workflows using n8n (rule-based and agent-driven automation) to correlate multi-platform alerts, reduce false positives, and accelerate mean time to response.
- Participated in proactive threat hunting exercises to identify indicators of compromise (IOCs) and suspicious lateral movement patterns across enterprise infrastructure.

Education

Mahatma Gandhi University (MGU) 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 CLI tool automating subdomain reconnaissance and intelligence correlation across VirusTotal API, WHOIS records, DNS lookups, and OSINT sources to map phishing infrastructure.
- Reduced manual investigation time for phishing domain analysis by consolidating workflows previously spread across multiple disparate tools – directly supporting faster analyst response.

Technical Skills

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

Certifications & Achievements

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