Dhananjay Krishnan K P

+91-8089983975 offcl.dhananjaykrishna@gmail.com dhananjay-krishna-k-p portfolio
Bengaluru, India

Professional Summary

EC-Council Certified SOC Analyst with 1+ year of hands-on experience in SOC operations, incident management, threat detection, phishing investigation, and playbook-based incident response within enterprise security environments. Experienced in monitoring and triaging security alerts, investigating malicious infrastructure, conducting IOC analysis, and coordinating phishing and brand abuse takedowns. Skilled in SIEM monitoring, threat hunting, OSINT-based investigations, security event correlation, and structured escalation workflows.

Professional Experience

SOC Analyst February 2025 – Present
Tikaj Technologies — Hunto AI *Remote, India*

- Monitored and investigated 5,000+ weekly security events involving phishing attacks, malicious applications, fake websites, and brand impersonation campaigns.
- Performed incident triage, IOC analysis, and threat detection activities within structured SOC operations workflows.
- Coordinated phishing and abuse takedown activities with registrars, hosting providers, and platform abuse teams to support rapid remediation of malicious assets.
- Followed playbook-based incident response procedures for phishing investigations, escalation handling, remediation coordination, stakeholder communication, and incident closure tracking.
- Improved incident classification and alert triage workflows, helping reduce false positives in a high-volume monitoring environment.
- Conducted weekly client calls with enterprise accounts across banking, fintech, e-commerce, and manufacturing sectors to provide incident updates and remediation status.
- Maintained timely response and remediation coordination for high-volume phishing and abuse incidents across multiple enterprise clients.

Cybersecurity Analyst Trainee (Part-Time Program) September 2025 – April 2026
Tracelay Networks Pvt Ltd *Remote, India*

- Completed a weekend-based part-time cybersecurity training program alongside full-time SOC Analyst responsibilities at HUNTO AI to gain hands-on experience with industry-standard SIEM, EDR and XDR platforms.
- Monitored and triaged security alerts across SIEM, NDR, EDR, and XDR platforms including Sumo Logic, ExtraHop, Trend Micro Vision One, and Cybereason.
- Investigated incidents using MITRE ATT&CK mapping to identify attack patterns, suspicious activity, and potential lateral movement.
- Participated in proactive threat hunting exercises to identify indicators of compromise (IOCs) and abnormal network behavior.
- Assisted in building AI-assisted triage workflows using n8n automation to improve alert correlation and reduce manual analysis effort.
- Supported incident response processes through investigation documentation, escalation workflows, and remediation coordination.

Cybersecurity Analyst Intern August 2024 – February 2025
RedTeam Hacker Academy *Calicut, Kerala, India*

- Gained hands-on experience with SIEM platforms including Splunk, Microsoft Sentinel, and IBM QRadar for log analysis and security monitoring.
- Performed packet analysis and network traffic investigation using Wireshark to identify suspicious behavior and indicators of compromise.
- Utilized Nmap, Nessus, Nikto, and Metasploit for vulnerability assessment and penetration testing activities in lab environments.
- Acquired hands-on experience with Burp Suite for web application security testing — performing vulnerability assessments including SQLi, XSS, IDOR, and other OWASP Top 10 attack vectors.
- Participated in multiple Capture The Flag (CTF) competitions, applying knowledge of reverse engineering, cryptography, web exploitation, and forensics to real-world challenge scenarios.
- Studied security frameworks including MITRE ATT&CK, NIST CSF, and Cyber Kill Chain.

Education

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

Security Projects

PhishRecon | *Phishing Infrastructure Reconnaissance Tool* | 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 — engineering security data collection into useful investigative insights.
- Reduced manual investigation time for domain analysis by consolidating workflows previously spread across multiple disparate tools, directly supporting faster SOC analyst response and abuse team coordination.

Technical Skills

SIEM & Security Monitoring: Splunk, Microsoft Sentinel, IBM QRadar, Sumo Logic NG-SIEM, IOC Analysis, Log Analysis, Alert Triage, Security Event Correlation, Security Documentation

Threat Detection & Incident Response: Incident Triage, Threat Detection, Threat Hunting, Root Cause Analysis, Escalation Workflows, Ticketing Systems, Playbook-Based Incident Response, Forensic Documentation

Threat Intelligence & OSINT: VirusTotal, WHOIS, DNS Analysis, Malicious Domain Analysis, OSINT Investigation, Threat Intelligence Analysis

Fraud & Abuse Investigation: Phishing Detection & Takedown, Brand Impersonation, Abuse Team Coordination, Vetting Abuse Claims

Network & Web Security Tools: Wireshark, Burp Suite, Nmap, Nessus, Nikto, Metasploit

Security Frameworks & Standards: MITRE ATT&CK, Cyber Kill Chain, NIST CSF, Incident Response Lifecycle

Automation & Scripting: Python, Bash, SPL, n8n Workflow Automation

Certifications & Achievements

EC-Council Certified SOC Analyst (CSA)

Certified IT Infrastructure & SOC Analyst (CICSA v3)

UGC NET Qualified – Computer Science